Search Report from Ginger D. Roberts

```
?show files;ds
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200318
         (c) 2003  Thomson Derwent
File 344:Chinese Patents Abs Aug 1985-2003/Jan
         (c) 2003 European Patent Office
File 347:JAPIO Oct 1976-2002/Nov(Updated 030306)
         (c) 2003 JPO & JAPIO
File 371:French Patents 1961-2002/BOPI 200209
         (c) 2002 INPI.  All rts. reserv.

Set     Items   Description
S1       1513   (ACCESS? OR "IS()AVAILABLE" OR "MADE()AVAILABLE")(5N)(EMBE-
            D? OR ENCOD? OR FINANCIAL OR IDENTIFICATION)(3N)(CONTENT? ? OR
             DATA OR INFORMATION)
S2        700   (CHALLENGE? OR RESPONSE)(5N)(VERIF? OR AUTHENTICAT?)
S3          5   S1 AND S2
```

?t3/4/all

3/4/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

IM- *Image available*
AA- 2002-257094/200230|
DX- <RELATED> 2002-105735; 2002-257121; 2002-749774; 2003-028628|
XR- <XRPX> N02-199057|
TI- Requesting and retrieving medical **information** for electronic **access** to medication, pharmaceutical and clinical **information** using subject **identification** to locate information|
PA- NEX2 LLC (NEXT-N); DICK R S (DICK-I)|
AU- <INVENTORS> DICK R S|
NC- 095|
NP- 003|
PN- WO 200198866 A2 20011227 WO 2001US19565 A 20010619 200230 B|
PN- AU 200168567 A 20020102 AU 200168567 A 20010619 200230
PN- US 20020194131 A1 20021219 US 2001883884 A 20010618 200303|
AN- <LOCAL> WO 2001US19565 A 20010619; AU 200168567 A 20010619; US 2001883884 A 20010618|
AN- <PR> US 2001883884 A 20010618; US 2000596810 A 20000619; US 2001794983 A 20010227|
FD- WO 200198866 A2 G06F-000/00
<DS> (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
<DS> (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW
FD- AU 200168567 A G06F-000/00 Based on patent WO 200198866|
LA- WO 200198866(E<PG> 58)|
DS- <NATIONAL> AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW|
DS- <REGIONAL> AT; BE; CH; CY; DE; DK; EA; ES; FI; FR; GB; GH; GM; GR; IE; IT; KE; LS; LU; MC; MW; MZ; NL; OA; PT; SD; SE; SL; SZ; TR; TZ; UG; ZW|
AB- <PN> WO 200198866 A2|
AB- <NV> NOVELTY - When a control server receives a request for medical information (105), it may optionally verify the request (110) before sending a **response** (125). The **verification** can be driven by the satisfaction of legal and security requirements and is communicated to the request handling software executing on the central server. The verification includes electronic verification of electronic watermarks or digital certificates submitted with the request.|
AB- <BASIC> DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for a program storage device with computer instructions, for a method of providing relevant medical data, for a method of determining location of patient records and for a method of electronically requesting medical information.
USE - Electronic accessing of medical, pharmaceutical and clinical information.
ADVANTAGE - Reduced likelihood of fraudulent obtaining of records.
DESCRIPTION OF DRAWING(S) - The drawing is a flow chart of the method.
pp; 58 DwgNo 2/10|
DE- <TITLE TERMS> REQUEST; RETRIEVAL; MEDICAL; INFORMATION; ELECTRONIC; ACCESS; MEDICATE; PHARMACEUTICAL; CLINICAL; INFORMATION; SUBJECT; IDENTIFY; LOCATE; INFORMATION|
DC- S05; T01|

IC- <MAIN> G06F-000/00; G06F-017/60|
MC- <EPI> S05-D06; S05-M; T01-C08A; T01-D01; T01-J05B3; T01-J06A1; T01-N01A2A; T01-N02B1B; T01-S03|
FS- EPI||

3/4/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

IM- *Image available*
AA- 2001-010392/200102|
XR- <XRPX> N01-007923|
TI- Connecting method for TCP/IP network for providing access to common dial-up user by driving remote computer or facilities to link to network from a remote computer|
PA- TIEN C (TIEN-I)|
AU- <INVENTORS> TIEN C|
NC- 002|
NP- 002|
PN- GB 2350259 A 20001122 GB 9911726 A 19990521 200102 B|
PN- CA 2272666 A1 20001121 CA 2272666 A 19990521 200103 N|
AN- <LOCAL> GB 9911726 A 19990521; CA 2272666 A 19990521|
AN- <PR> GB 9911726 A 19990521; CA 2272666 A 19990521|
LA- GB 2350259(32); CA 2272666(E)|
AB- <PN> GB 2350259 A|
AB- <NV> NOVELTY - The method is implemented by a network connection control server providing access to a TCP/IP computer network (5) through a remote computer connected to network control server (7). The TCP/IP computer network is located remotely and enables the remote computer to actively access the destination computer over the TCP/IP computer network.|
AB- <BASIC> DETAILED DESCRIPTION - The method involves: (a) receiving log-on identification information sent by a user (1) from the remote computer to the network connection control server, wherein the log-on identification information verifies that the user can perform a remote control for connection by means of the network connection control server; (b) in **response** to **verifying** the log-on **identification information** , the network connection control server attempting to **access** the destination computer through an assigned connection **identification information** ; (c) in response to receiving the connection identification information, initiating a connection between the network connection control server and the destination computer; (d) sending the identification information to the destination computer; (e) in **response** to **verifying** the identification information, providing an assigned IP address to the destination computer, which utilizes the assigned IP address to communicate over the TCP/IP computer network; (f) connecting the destination computer to the TCP/IP computer network, and receiving a safe connection acknowledgment from the destination computer; and (g) in response to the safe connection acknowledgement, sending the IP address assigned to the destination computer to the remote computer, and using the IP address to connect the remote computer to the destination computer over the computer network. An INDEPENDENT CLAIM is also included for a computer readable recording medium which records an indirect connecting method.

USE - For enabling a remote user at a remote computer to access a computer selectively connected to a local computer network.

ADVANTAGE - Provides a common dial-up user for dialing up the TCP/IP network using a network connection control server coupled to the network to actuate the remote computer or the connection device, thus enabling the user to access data from the remote computer as well as executing the disconnection procedure after the access is completed.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic view of a network connection for a remote dial-up direct connection.
User (1)
Destination computer (2)
Modem (3,9)
TCP/IP network (5)
Remote node (6)
Control server (7)
User connection database (8)
PSTN (10)
pp; 32 DwgNo 3A/6|
DE- <TITLE TERMS> CONNECT; METHOD; IP; NETWORK; ACCESS; COMMON; DIAL; UP; USER; DRIVE; REMOTE; COMPUTER; FACILITY; LINK; NETWORK; REMOTE; COMPUTER|
DC- T01; W01|
IC- <MAIN> H04L-012/12; H04L-012/66|
MC- <EPI> T01-H07C5E; T01-J05B4P; T01-M02A1C; T01-S03; W01-A06G3|
FS- EPI||

3/4/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

IM- *Image available*
AA- 1996-489940/199649|
XR- <XRPX> N96-412872|
TI- Communication system e.g. client-server system connected to computer network - includes access **response** appts. so that session **authentication** data might be used and user authentication of access demand appts. might be performed|
PA- FUJITSU LTD (FUIT)|
NC- 001|
NP- 001|
PN- JP 8249253 A 19960927 JP 9552383 A 19950313 199649 B|
AN- <LOCAL> JP 9552383 A 19950313|
AN- <PR> JP 9552383 A 19950313|
FD- JP 8249253 A G06F-013/00|
LA- JP 8249253(9)|
AB- <BASIC> JP 8249253 A
The system has access demand devices (1) which send a user authentication data of an access demand to access response device (2) in connection with a session to perform. When the access response appts. permits the access of the access demand appts. by the user **authentication** , the access **response** appts. is restricted to the session and publishes an effective session authentication data.
The session authentication data is sent to the access response appts., generated by the time the session ends the access demand appts. The access response appts. is included so that the session authentication data might be used and user authentication is performed.
USE/ADVANTAGE - E.g. local area network, wide area network for world wide web or hyper text markup language. Performs user authentication on access demand appts. corresp. to **access** demand. Secures **data** on server even when session **identification** or pass word is stolen. Reduces probability of unauthorised use in original ID or original pass word.
Dwg.2/6|
DE- <TITLE TERMS> COMMUNICATE; SYSTEM; CLIENT; SERVE; SYSTEM; CONNECT; COMPUTER; NETWORK; ACCESS; RESPOND; APPARATUS; SO; SESSION; AUTHENTICITY; DATA; USER; AUTHENTICITY; ACCESS; DEMAND; APPARATUS; PERFORMANCE|
DE- <ADDITIONAL WORDS> WWW; HTML; LAN; WAN|

DC- P85; T01; W01|
IC- <MAIN> G06F-013/00|
IC- <ADDITIONAL> G06F-001/00; G09C-001/00; H04L-009/32; H04L-012/00|
MC- <EPI> T01-H07C; W01-A05B; W01-A06E2A|
FS- EPI; EngPI||

3/4/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

IM- *Image available*
AA- 1991-051555/199108|
XR- <XRPX> N91-039949|
TI- Authenticating call seeking access to vendor-provided services - using intelligent network as part of carrier telephone switching system, has database contg. identities of bona-fide customers|
PA- AMERICAN TELEPHONE & TELEGRAPH CO (AMTT); AT & T BELL LAB (AMTT)|
AU- <INVENTORS> MEDAMANA J B; PALMER J W; WEBER R P|
NC- 002|
NP- 003|
PN- CA 2013374 A 19901130 CA 2013374 A 19900329 199108 B|
PN- US 5181238 A 19930119 US 89359823 A 19890531 199306
PN- CA 2013374 C 19931130 CA 2013374 A 19900329 199403|
AN- <LOCAL> CA 2013374 A 19900329; US 89359823 A 19890531; CA 2013374 A 19900329|
AN- <PR> US 89359823 A 19890531|
FD- US 5181238 A H04M-011/00
FD- CA 2013374 C H04M-003/42|
LA- US 5181238(13)|
AB- <BASIC> CA 2013374 A

Intelligent network facilities are used as part of a common carrier telephone switching system. The intelligent network comprises a data base which contains all customer identities or account numbers received from a service provider which are to be entitled to access the vendor services. A caller requesting service dials the number of the service provider. For some applications, the caller's telephone number is recognised by automatic number identification (ANI). The call is connected to a toll switching system equipped with a network services complex for requesting the customer to key an account number (where appropriate if the ANI number is not an adequate identification or if the customer is calling from a different telephone station) and a personal identification number (PIN).

The toll switching system that accesses a data base to verify if the customer identified by the ANI number and/or the account number, further authenticated by the PIN number or other suitable **identification data** , is authorised to **access** the service provider. If so, the call is connected to the service provider who need not perform further authentication.

USE/ADVANTAGE - Electronic mail, facsimile and computer generated data. Only one PIN number needed. (23pp Dwg.No.1/6|

AB- <US> US 5181238 A

The method involves a switching office, responsive to receipt of a call comprising a called number identifying the destination, data identifying a caller, and authentication data, querying a data base for accessing data, using the called number. The identifying data and the authentication data verify authentication of the caller and authorisation by the destination of access by the caller.

In **response** to a positive **verification response** from the data base the call is extended toward the destination. The data identifying the caller comprises an automatically identified telephone number.

ADVANTAGE - Caller need only remember one PIN for all service providers accessed by arrangement.
Dwg.1/6|
DE- <TITLE TERMS> AUTHENTICITY; CALL; SEEKER; ACCESS; VENDING; SERVICE; INTELLIGENCE; NETWORK; PART; CARRY; TELEPHONE; SWITCH; SYSTEM; CONTAIN; IDENTIFY; CUSTOMER|
DE- <ADDITIONAL WORDS> ELECTRONIC; MAIL; FACSIMILE|
DC- W01|
IC- <MAIN> H04M-003/42; H04M-011/00|
MC- <EPI> W01-A06X; W01-C02B; W01-C05B1; W01-C05B3; W01-C05B5|
FS- EPI||

3/4/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

AA- 1979-H6012B/197936|
TI- Automatic cash dispensing machine - uses terminal **data** storage and enables **access** to master **data** storage when customer **identification** card **data** is cleared|
PA- IBM CORP (IBMC)|
AU- <INVENTORS> ANDERSON R W; BROCK S F; GEE M L|
NC- 010|
NP- 006|
PN- EP 3756 A 19790905 197936 B|
PN- US 4186871 A 19800205 198007
PN- CA 1103352 A 19810616 198129
PN- EP 3756 B 19810916 198139
PN- DE 2960795 G 19811203 198150
PN- IT 1164986 B 19870422 198934|
AN- <PR> US 78882529 A 19780301|
CT- US 3394246; US 3696335; US 3727186; US 4016405; US 4023013; 1.Jnl.Ref|
FD- EP 3756 A
<DS> (Regional): BE CH DE FR GB NL SE
FD- EP 3756 B
<DS> (Regional): BE CH DE FR GB NL SE|
LA- EP 3756(E); EP 3756(E)|
DS- <REGIONAL> BE; CH; DE; FR; GB; NL; SE|
AB- <BASIC> EP 3756 A

A transaction execution system is for use, e.g. at a cheque cashing machine. It includes a transaction terminal (1) for approval of a transaction and a host data processing system (11) in communication with the terminal. The latter includes a storage device (10) for storing a set of issuer-unique control blocks each including coding key.

The terminal includes a store (8) storing a smaller set of issuer-unique control blocks each including coding key. A card reader (2) is provided t read encoded data on an identification card presented to the terminal by a user. The data includes issuer identification and card **verification** data. In **response** to the former the terminal store is searched for a corresponding control block and, if none is found, encoded data is communicated to the hose.

The system provides a self-service facility for bank customers available twenty-four hours per day. A magnetic stripe card with encoded identification data is issued to the customer for use at the terminal to initiate a transaction, his/her identity being further verified by a personal identification number (PIN) which he enters at the terminal keyboard. The identification data is enciphered for security. Coding and decoding is carried out by an encoding algorithm and the banks' secret encoding keys|
DE- <TITLE TERMS> AUTOMATIC; CASH; DISPENSE; MACHINE; TERMINAL; DATA;

STORAGE; ENABLE; ACCESS; MASTER; DATA; STORAGE; CUSTOMER; IDENTIFY; CARD; DATA; CLEAR|
DC- T01; T04; T05; W01|
IC- <ADDITIONAL> G06F-015/30; G06K-005/00; G07C-011/00; H04Q-003/54|
FS- EPI||
?

Search Report from Ginger D. Roberts

```
?show files;ds
File   2:INSPEC 1969-2003/Mar W2
         (c) 2003 Institution of Electrical Engineers
File  35:Dissertation Abs Online 1861-2003/Feb
         (c) 2003 ProQuest Info&Learning
File  65:Inside Conferences 1993-2003/Mar W3
         (c) 2003 BLDSC all rts. reserv.
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Feb
         (c) 2003 The HW Wilson Co.
File 233:Internet & Personal Comp. Abs. 1981-2003/Feb
         (c) 2003 Info. Today Inc.
File 256:SoftBase:Reviews,Companies&Prods. 82-2003/Feb
         (c)2003 Info.Sources Inc
File 474:New York Times Abs 1969-2003/Mar 18
         (c) 2003 The New York Times
File 475:Wall Street Journal Abs 1973-2003/Mar 18
         (c) 2003 The New York Times
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group

Set     Items   Description
S1        943   (ACCESS? OR "IS()AVAILABLE" OR "MADE()AVAILABLE")(5N)(EMBE-
              D? OR ENCOD? OR FINANCIAL OR IDENTIFICATION)(3N)(CONTENT? ? OR
               DATA OR INFORMATION)
S2       1130   (CHALLENGE? OR RESPONSE)(5N)(VERIF? OR AUTHENTICAT?)
S3          0   S1 AND S2
?
```

```
?show files;ds
File  15:ABI/Inform(R) 1971-2003/Mar 18
         (c) 2003 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2003/Mar 18
         (c) 2003 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2003/Mar 18
         (c)2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2003/Mar 18
         (c) 2003 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2003/Mar 18
         (c) 2003 The Gale Group
File   9:Business & Industry(R) Jul/1994-2003/Mar 18
         (c) 2003 Resp. DB Svcs.
File  20:Dialog Global Reporter 1997-2003/Mar 19
         (c) 2003 The Dialog Corp.
File 476:Financial Times Fulltext 1982-2003/Mar 19
         (c) 2003 Financial Times Ltd
File 610:Business Wire 1999-2003/Mar 19
         (c) 2003 Business Wire.
File 613:PR Newswire 1999-2003/Mar 19
         (c) 2003 PR Newswire Association Inc
File 624:McGraw-Hill Publications 1985-2003/Mar 18
         (c) 2003 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2003/Mar 18
         (c) 2003 San Jose Mercury News
File 636:Gale Group Newsletter DB(TM) 1987-2003/Mar 18
         (c) 2003 The Gale Group
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc

Set     Items   Description
S1      48886   (ACCESS? OR "IS()AVAILABLE" OR "MADE()AVAILABLE")(5N)(EMBE-
           D? OR ENCOD? OR FINANCIAL OR IDENTIFICATION)(3N)(CONTENT? ? OR
            DATA OR INFORMATION)
S2       6493   (CHALLENGE? OR RESPONSE)(5N)(VERIF? OR AUTHENTICAT?)
S3         40   S1 AND S2
S4          2   S1(S)S2
S5        245   S2 AND (BIOMETRIC? OR BIO()METRIC? OR IRIS OR EYE OR EYES)
           AND (PIN OR PERSONAL()IDENTIF?(2W)(NUMBER? OR CODE?) OR PASSC-
           ODE? OR PASSWORD? OR PASS()CODE? OR PASS()WORD?)
S6          9   S1 AND S5
S7        175   S5 NOT PY>2000
S8          7   RD S6 (unique items)
S9      37763   (USER OR OWNER)(3N)(VERIF? OR AUTHENTICAT?)
S10        95   S7 AND S9
S11        55   RD (unique items)
?
```

?t8/3,k/all

8/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00621996 92-37098
Trusted Products Evaluation
Chokhani, Santosh
Communications of the ACM v35n7 PP: 64-76 Jul 1992
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 6863

...TEXT: accountability.

AUTHENTICATION. This feature allows the TCB to authenticate the user's identity. Examples of **authentication** mechanism include **passwords** (6), **biometrics** , **challenge** -response devices (5), etc. In many breakins, we hear that the key weakness has been the ability to compromise the intent of the authentication mechanism by guessing **passwords** . It is very critical to have a protected authentication mechanism that cannot be easily compromised...

...interrupt the login sequence to steal a user (e.g., power on, break key) or **password**). It can be implemented character sequence from the terminal as a request for communications with...that is why C2 is considered the minimum to protect ADP systems that process sensitive **information** . CONTROLLED **ACCESS** PROTECTION (Class C2). In this class **identification** , authentication, DAC, and auditing are required at the individual user level. Object reuse protection is...D.E. Cryptography and Data Security. Addison-Wesley, Reading, Mass., 1983.

6. Department of Defense. **Password** Management Guidelines. CSC-STD-002-85, April 1985.

7. Department of Defense. Trusted Computer System...

8/3,K/2 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05903931 Supplier Number: 53119818 (USE FORMAT 7 FOR FULLTEXT)
REMOTE POSSIBILITIES FOR THE ENTERPRISE.(Company Operations)
Network, p97(1)
July 1, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 3216

... an authentication server. Users log in with a login ID, which generates a unique alphanumeric **password** every 60 seconds. For one more level of security, encrypted tunnels will be developed between...North America, and Asia Pacific.

To access their sites over the Internet, partners have a **password** that is changed frequently. The HP 9000 Unix-based servers have built-in security, but...

...Hamilton.

Through EBF, select customers can tap into a range of specially tailored, for-their **eyes** -only Web pages. The information provided on these pages ranges from a listing of what...

...eligibility.
To access EBF, Hamilton says customers "only need to register once, maintain one secure **password** , and have one hole in their firewall for delivery of services." But there are other...

...is to have multilayers of security--depending on the level of service. Beyond the basic **password** , a user's ability to tap into the main **access** level of **information** is restricted by domain **identification** ; in other words, what services are available depends on whether the user is accessing EBF...

...the same security issues regardless of the switch or vendor we used," Brandt explains. "The **challenge** is getting the **authentication** part right, and we haven't fully worked through those issues; this is why we...

8/3,K/3 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04968096 Supplier Number: 47299582 (USE FORMAT 7 FOR FULLTEXT)
SPEECH VERIFICATION PROVES TO BE A STEAL
Voice Technology & Services News, v16, n8, pN/A
April 15, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1095

... to look for is redundancy at different levels that tightens security at different levels. Voice **biometrics** is perfect for that."
Biometrics is a security technology that identifies an individual based on biological traits such as fingerprinting, handwriting, retinal scans, face scans or speech verification. Voice **biometrics** identifies a live voice with a previously recorded voice print.
The Pros of Voice **Biometrics**
Among the **biometric** technologies, speech verification is among the newer ones. While no **biometric** measure is 100 percent accurate, speech vendors are touting advantages to speech verification by saying...

...Strengthening Voice Security
Most forms of transacting sensitive information require a user to enter a **personal identification number** (**PIN**) or **password** , whether it is to make a long- distance call or **access** bank account **information** . Such forms of **identification** authenticate a computer, a card, a keyboard, but not a person, says Jason McDermit, vice...

...where hackers could crack security systems. While it is true that fraudulent users can steal **PIN** numbers, **passwords** and other forms of identification, they cannot steal a person's voice. But they have...

...that includes automating the process after the identity of the caller is verified."
"Overlaying voice **authentication** into interactive voice **response** systems is a great idea, especially in niche markets where voice authentication is getting good...

...it traverses the network.
Swansea, Mass.-based ImagineNation bases its speech verification technology on a **password** that is stored on a card as "voice print data." Direct analog storage allows use increasing
speech combinations.
False Rejections: * Vendors are teaming speech

verification with interactive voice **response** systems to provide an alternate route for failed voice attempts. "It's like touch-tone...

...manager for
Pleasanton, Calif.-based Votan Corp., a speech verification company. "If you input your **personal identification number** incorrectly of if you lose your number, you have to go to a live operator...

8/3,K/4 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10708512 SUPPLIER NUMBER: 53437157 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Finger imaging at automated branches makes Purdue Employees FCU a pioneer in biometric **security.(Purdue Employee Federal Credit Union)**
Koehler, Gail J.
Journal of Retail Banking Services, 20, 4, 13(5)
Winter, 1998
ISSN: 0195-2064 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2557 LINE COUNT: 00204

Finger imaging at automated branches makes Purdue Employees FCU a pioneer in biometric **security.(Purdue Employee Federal Credit Union)**

...ABSTRACT: Federal Credit Union is the first financial services institution in North America to successfully apply **biometrics** for ensuring security of remote access of accounts at automated teller machines (ATMs). Cooperative efforts...

...Inc of Norfolk, VA, resulted in TARA (Technologically Advanced Remote Access) Touch ATMs which use **biometric** finger imaging for confirming identity instead of the usual **personal identification numbers** .
TEXT:
When we made the decision to use **biometrics** at our TARA Touch units, we started educating our members about **biometrics** immediately, emphasizing the security features it would add to our members' accounts.
... union was the first financial institution in North America to successfully implement the use of **biometrics** for secure account access at remote locations. The use of **biometrics** came about as a result of our need to serve members outside our original geographic...

...to our members at remote locations - which, in turn, led to our pioneering applications of **biometric** technology for security purposes.
When we began to look for ways to grow, we already...

...us to Real Time Data Management, Inc., in Norfolk, Virginia.
TARA Touch Automated Branching - Protected **Biometrically**
We worked closely with them, and in February 1997, they delivered our first TARA (Technologically...

...members to access their accounts remotely.
According to Jim Wayman, the director of the National **Biometric** Test Center at Stanford University in Palo Alto, California, " **Biometrics** (is) the automatic identification or identity verification of individuals based on behavioral or physiological characteristics." The staff at Real

Time Data convinced us to use **biometrics** for more secure account access on TARA Touch. They believe that **biometrics** is the future of security for remote account access and have developed a very user...

...for use on the units. Collaborating with National Registry Inc., they worked to add a **biometric** identification module for secure account access on the system.

Biometrics can be used either for verifying the identity that someone is claiming, using a one...

...is identified with no prior claimed identity. In PEFCU's current application, we are using **biometric** finger imaging as a means of positively verifying our members' identity. We are replacing the use of **personal identification numbers** (PINs) with **biometric** verification.

With the verification process we are using, it is still necessary for members to...

...number when accessing their funds at TARA Touch. In the future, we plan to use **biometric identification** to allow members to **access** their account **information** without the necessity of entering an account number.

Today, at a TARA Touch branch, any...

...our credit union using the touch screen technology of TARA Touch without the use of **biometric** identification. Anyone eligible for membership can open an account and the **biometric** registration occurs during the account opening process.

Economic Advantages, Too. Besides the added security the use of **biometrics** provides to our members, the TARA Touch program makes a lot of sense to a...

...of a supermarket branch like the one we have at the Calumet campus.

Additionally, a **biometric** identifier cannot be lost or stolen as a **PIN** can be, and, if we accomplish our goal of replacing card access with **biometric** access, there will be no lost, damaged, or stolen cards to replace - nor will it 1980s - requires the use of a **PIN** number; we have found that when members have problems accessing that system due to **PIN** failure, they blame themselves. They assume they have mis-keyed or forgotten the number. When...

...but not necessarily with the system. Consumers view card services as a proven, reliable technology. **Biometrics** is, however, newer and so less trusted; if a member has trouble using **biometrics** , he almost always blames the system first.

For this reason, we have placed great importance on member education. As the use of **biometrics** for identification and verification becomes more common in the marketplace, I believe we will see as good consumer acceptance of **biometrics** as we now have of cards and PINs.

To ensure the success of TARA Touch...

...the units. We have also made sure we have backup systems in place for the **biometric** process in the event that the member has a problem accessing his or her account...

...case of hardware failure (finger scanner failure, etc.), the member can use the TARA Talk **PIN** that we use as one of the identifiers when we register the member's finger...

...their accounts.

Finally, it is very important that the user see the benefit of using **biometrics** in place of more traditional **verifiers** for their account access. The **response** we've gotten has been impressively positive, with members quickly recognizing the high level of...

...the consumer will use and/or accept it. When we made the decision to use **biometrics** at our TARA Touch units, we started educating our members about **biometrics** immediately, emphasizing the security features it would add to our members' accounts.
Initially, we thought...

...Touch units over the same period of time.
Learning ...
We have learned a lot about **biometrics** - and we are still learning. The fact that most of our members are technologically proficient...for our fourth live installation, we've been constantly updating the program and learning about **biometrics** and how it can best be utilized at our credit union.
At PEFCU, we foresee many other possible applications for **biometrics** - such as building access, ATM access, verification of web-based home branch users, and credit...

...system in our new Administrative Building and Financial Mall that we plan to retrofit with **biometric** access in the relatively near future and have signed an agreement with TRW to pilot...

...providing account access with identification rather than verification as one of our primary goals for **biometrics** .
We feel that **biometrics** has offered our credit union a good solution to the problem of how to provide...
...Responsible for the research and development of new technology, she has written several articles about **biometrics** and remote automated branching and has testified before the House Banking Committee on the topic.

8/3,K/5 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

03933571 SUPPLIER NUMBER: 07494095 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Who goes there? (user-verification systems to restrict access to computer data) (special section - Computer-Information Security: Getting the Protection You Need)
Mayfield, Charles
Security Management, v33, n2, p36A(3)
March, 1989
ISSN: 0145-9406 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2007 LINE COUNT: 00164

... systems for computers in network environments: logic-based systems, hand-held key token devices, and **biometric** systems. Each system functions by confirming that the user who wants to gain access to...

...fact, authorized to gain access.
Logic-based systems. These are typically software-based systems using **passwords** that rely on what a user knows to determine authentication. While easy to implement, **password** systems are very difficult to secure. For one thing, **passwords** can be fairly simple to decipher. People often use names, anniversary dates, and other **passwords** that are easy for the user to remember--and also easy for someone else to figure out.
In addition, users write **passwords** down so they don't forget them. Once written, the **password** may be seen by anyone and, once public, all protection is lost. Repeated use of the same **password** and the sharing of **passwords** among users also threaten their effectiveness.
For management and administration, **password** security systems can be more trouble than they are worth. Management must assign and eliminate **passwords** to keep pace with employee turnover. They may also want to issue

multiple IDs to grant individual users special privileges, depending on their job functions.

An extended **password** algorithm system offers an alternative to memorized **passwords** , but it also is difficult to administer. In an algorithm-based security system, the user...

...is "dog."

In the algorithm system, each challenge is unique, so the problem of exposing **passwords** is limited. However, administration of the algorithm system is cumbersome and raises some difficult questions...

...are programmable, hand-held devices, which are used in conjunction with a user ID and **password** . A separate key is assigned to each user. Then, when software on the host computer issues a challenge, the key is used to provide a proper **response** .

In one particular key token **authentication** device system, the host issues a challenge via a flashing light pattern that represents a...

...the flashing pattern, read and process the random number. The access key then displays a **password** on its LCD screen. The user enters this **password** on the computer terminal keyboard. If the correct key has been used for the corresponding...

...granted.

One of the benefits of this system is that the software generates a unique **password** with each use, making it impossible for a user to guess a **password** . The key will operate on mainframes, minicomputers, and PCs.

In addition, management can allow a...

...specific data bases, applications, and networks.

The token key approach provides greater security than the **password** approach and is suitable in settings that require moderate levels of security and in mobile...

...used to protect a company's proprietary product information, financial data, and consumer market information.

Biometric authentication systems. These systems provide the highest level of security. They incorporate hardware and software...

...corporate accounting records. Corporations with large, centralized data bases are becoming more common users of **biometric** security systems.

Active **biometric** systems analyze the user's personal characteristics to determine whether access is permissible. Characteristics such...

...unique to the individual; they cannot be stolen, forgotten, written down, misplaced, or duplicated. Hence, **biometric** systems that use these characteristics provide an extremely high level of security. Passive **biometric** systems analyze characteristics related to behaviors to authenticate user ...the data, and compares it to the stored fingerprint data.

From an administrative perspective, a **biometric** system requires minimal management. Unlike the **password** system where the user must routinely protect and change his or her **password** , a **biometric** characteristic will not change, so user IDs do not have to be changed periodically. (However...

...mistakenly grants access to an unauthorized user, and false denials were a problem for early **biometric** systems. Today's technology has improved on the accuracy of early versions. However, the technology...

...be successful, the company's needs and the effectiveness of each

technology should be considered. **Passwords** , token devices, and **biometrics** provide different levels of security. It is not necessary to purchase a high-level security...

...These factors should be considered for any extended user authentication system, whether token-based or **biometric** .

First, define precisely what should be protected and to what degree. Should all organizational **data** be protected or only **financial information** ? Distinguish which personnel will be allowed **access** to which types of data. Perhaps senior management should be granted access to all data...

...A mix of authentication systems may be most appropriate. A combination of token systems and **biometrics** provides a higher level of security. Or, different technologies may be applied to computers that...

...with access to organizational data make in-house data bases and networks vulnerable to tampering.

Password protection may be the solution, or it may be too vulnerable and labor-intensive for...

...provide a higher level of security and are particularly well suited for dial-up networks. **Biometrics** provide the highest level of user verification and can not only augment but in some cases actually replace **password** protection.

Whichever solution the company chooses, the most important point is to secure access to...

8/3,K/6 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02418496 SUPPLIER NUMBER: 62266765 (USE FORMAT 7 OR 9 FOR FULL TEXT)
2000 Products of the Year Award Winners.
Network Magazine, NA
May 1, 2000
ISSN: 1093-8001 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 12704 LINE COUNT: 01053

... screen-popping using any phone and a PC running Windows 95 or above. Voicemail is **accessed** through Microsoft Outlook, while Caller Line **Identification** (CLI) **information** is automatically crossreferenced to the Outlook directory so that a caller's name is displayed...order to talk, customers and vendors have to negotiate a bevy of firewalls, VPN clients, **password** dialogs, certificate infrastructures, and more.

The vision driving adoption of directories is that, once they...

...was hence acquired by Legato Systems.)

The product still has the features that caught our **eye** last year- bidirectional failover, the option of both active/active and active/passive configurations, well...PKI compatible.

The system includes support for many companies' digital certificates. It also supports Remote **Authentication** Dial-In User Service (RADIUS), **Challenge** Handshake **Authentication** Protocol (CHAP), and **Password** Authentication Protocol (PAP), as well as RSA's SecurID tokens.

www.vpnet.com
Authentication
ClearTrust...

...SecureControl includes a single sign-on capability and supports multiple authentication methods, such as username/ **password** , digital certificates,

and tokens. Permissions can be established at the server, directory, application, or Web...for signs of an intrusion. Host-based systems monitor specific local machines and keep an **eye** out for activity that deviates from predefined parameters.

RealSecure 3.2 from Internet Security Systems...including digital signatures, RSA encryption, server authentication prior to transmission, a document expiration date, and **password** protection. In addition, the Tumbleweed IME developer toolkit lets in- house developers customize IME-enabled...

8/3,K/7 (Item 1 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

22749748 (USE FORMAT 7 OR 9 FOR FULLTEXT)
How to keep intruders away: Mohan Bhatia on ensuring computer security through access controls
BUSINESS LINE
May 13, 2002
JOURNAL CODE: FBLN LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 2020

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... are further divided into preventive and detective physical controls. Preventive controls include: locks and keys; **biometric** access controls; tokens; back-up of files and documentation; and environment controls.

Locks and keys...

... have tamper-detection circuits, which erase the secure key storage, if the circuit is broken.

Biometric locks: Doors and entry locks that are activated by **biometric** features such as the voice, **eye** retina scan, fingerprint or signature.

Biometric techniques

Biometric devices are the latest addition to the physical security, as a baseline measure. **Biometric** techniques also work as a logical access control.

Every person is unique. **Biometrics** is the use of physical traits and characteristics of a person to provide positive personal...

... hundreds of years, fingerprints have been used as a means to provide individual identity. Computerised **biometric** techniques examine a specific physical trait to authenticate the user. **Biometric** systems which examine fingerprints, handprints, retina pattern, voice patterns and signatures are available in the market. **Biometric** equipment and techniques have not become popular because of high cost and high rejection rates.

Biometric controls are computer-based security methods that measure physical traits and characteristics such as fingerprints, voice, retina, keystroke dynamics. **Biometrics** is used for personal trait based authentication.

All **biometric** devices operate in a similar manner. Users are enrolled or registered, and allotted an identification number, name or other identifier. A **biometrics** sample is then submitted to the system (physical traits). The sample is processed and stored...

...template. Subsequent to registration, each authorised user enters his or her identity and submits the **biometric** sample. The device, then verifies the claimed identity, by comparing the enrolled profile of the...

... measurement of the attribute derived from the individual who seeks

access.
Areas of concern: Integratability: **Biometric** devices are stand-alone pieces of hardware, with functionality hard coded within the firmware. The ...

...allow much integration with application or hardware.
High cost: Capital and operating cost of the **biometric** system is still very high.
Maintainability: This is a new and complex technology. In-house maintenance of the **biometric** system is difficult.
False rejection rates: The biggest determinant of the success of a system...
... to authenticate his/her identity. The device may be token cards, card readers or a **biometric** device. All of them have the same purpose, that is, to authenticate the user to...

... employee ID badges, picture along with the individual's statistics - supplies enough information for the **authentication** process to be complete.
Challenge response tokens: Challenge response tokens supply **pass - codes** that are generated using a **challenge** from the process requesting **authentication** . Users enter their assigned user IDs and **passwords** , plus a **password** supplied by the token card. This process requires that the user supplies something they possess (the token) and something they know (the challenge-response process). This makes **pass - code** sniffing and brute force attacks futile.
Smart cards: A smart card contains microchips that consist...

... network for authentication. The ATM card requires the user to enter a personal ID number (**PIN**) along with the card, to gain **access** . The ATM compares the **information encoded** on the smart card with the information entered in the ATM machine.
Backup procedures
A...
?

?t11/3,k/all

11/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02061392 59191447
Voice biometrics
Markowitz, Judith A
Association for Computing Machinery. Communications of the ACM v43n9 PP: 66-73 Sep 2000
ISSN: 0001-0782 JRNL CODE: GACM
WORD COUNT: 4231

Voice biometrics
...TEXT: recognition tasks with such technologies as speaker verification and speaker identification. Like human listeners, voice **biometrics1** use the features of a person's voice to ascertain the speaker's identity. Systems...

... focusing on deployed, real-world technologies and the types of applications being used today.

Voice- **biometrics** systems can be categorized as belonging in two industries: speech processing and **biometric** security (see Figure 1). This dual parentage has strongly influenced how voice- **biometrics** tools operate in the real world.
Speech processing. Like other speech-processing tools, voice **biometrics** extract information from the stream of speech to accomplish their work. They can be configured...

... speech recognition, they benefit from lots of data, good microphones, and noise cancellation software. Voice **biometrics** are vulnerable to some of the same conditions that cause speechrecognition systems to perform poorly...

...telephones; and extreme hoarseness, fatigue, or vocal stress.

There are also important differences between voice-- **biometrics** systems and other speech-processing technologies, including speech recognition. The most significant is that voice **biometrics** technologies do not know what a person is saying, relying on speech recognition to do that. Moreover, the trend toward speaker independence that characterizes speech recognition cannot exist for voice **biometrics** . By definition, voice **biometrics** are always linked to a particular speaker. As a result, they require some type of enrollment for each user. The need for enrollment is an attribute voice **biometrics** shares with its relatives in the **biometric** -security industry.
Biometric security. Membership in the **biometrics** industry influences how voice- **biometrics** systems are used. **Biometrics** -based technologies are applied most often in security, monitoring, and fraud prevention where they positively identify individuals and distinguish one person from another. These abilities differentiate **biometrics** from all other forms of automated security. A card system can, at best, determine only whether a person has a viable access card, and **password** security can determine only whether the person knows the proper **password** . None of them verify that the person presenting the card or entering the **password** is the individual authorized to do so.

Biometric systems determine whether a **biometric** sample, such as a fingerprint or spoken **password** , comes from a specific individual by comparing that sample with a reference **biometric** --a sample of the same

type of **biometric** provided by the individual in question. Developers of voice **biometrics** called this a "reference voiceprint." As with reference templates for other **biometrics** , reference voiceprints are evaluated in terms of the number of times they mistakenly accept a...

...times they reject a legitimate speaker as an impostor.

The most significant difference between voice **biometrics** and other **biometrics** is that voice **biometrics** are the only commercial **biometrics** that process acoustic information. Most other **biometrics** are image-based. Another important difference is that most commercial voice **biometrics** systems are designed for use with virtually any standard telephone on public telephone networks. The...

... work with standard telephone equipment makes it possible to support broad-based deployments of voice **biometrics** applications in a variety of settings. In contrast, most other **biometrics** require proprietary hardware, such as the vendor's fingerprint sensor or **iris** -scanning equipment. This distinction-standard versus proprietary input device-is beginning to disappear. The recent...

... quality cameras, for example, now enables wider deployment of face-recognition applications.

Types of Voice **Biometrics**

The following sections outline the best-known commercialized forms of voice **biometrics** : speaker verification and speaker identification.

Speaker verification. Speaker-verification systems authenticate that a person is...

... of interacting with speaker-verification systems. Most commercial systems are text-dependent. They request a **password** , account number, or some other prearranged code. Because it requests a **password** , the system in Figure 3a is text-dependent. Text-dependent systems provide what the data... the correct voice (an example of "Who you are" security) and also know the proper **password** (an example of "What you know" security).

The system in Figure 3b displays a text-dependent, voice-only approach that uses the account number as both identity claim and **password** . Speech recognition decodes the input, and speaker verification uses the same input as the **biometric** sample it compares to the reference voiceprint.

Figure 3c shows an example of "text-prompted...

... voiceprint it generates must contain all the components that will be used to construct challenge- **response** variants. As Figure 3c indicates, **verification** also takes longer.

Text prompted verification is well-suited to highsecurity and high-risk systems...
... a result, creating a recording that can fool these systems is a difficult and costly **challenge** .

Text-independent **verification** accepts any spoken

Figure 3.

input, making it possible to design unobtrusive, even invisible, verification...

...phone.

Figure 4.

Table 1.

Enhancing performance. As in speech recognition, the performance of voice- **biometrics** systems is adversely affected by noise in the telephone channel and by other acoustic variability...

...models of network noise into complex, data-rich speaker-independent word models. By contrast, voice **biometrics** work with speaker-dependent models created from a limited amount of data spoken on a...cohort modeling identify individuals whose voices are similar to the voice of a newly enrolled **user** . During **verification** , the system compares the new input to each of the cohorts, as well as to...

...other people--even in adverse conditions.

Commercial Applications and Trends

Most commercial applications of voice **biometrics** provide security, fraud prevention, or monitoring; see Table 1 for a partial list of deployed...

... They also reflect the diversity and creativity being applied to real-world implementations of voice **biometrics** .

Data security (Illinois Department of Revenue). The Illinois Department of Revenue (IDOR) is the taking...

... privacy, Girl Tech incorporated chip-based text-dependent speaker verification into its Door Pass and **Password** Journal products. Door Pass is a brightly colored plastic device that attaches to a bedroom... ...sensor by pressing the on/off button; whenever the door moves, Door Pass demands the **password** . If the proper **password** is not supplied in the correct voice, Door Pass registers an intruder and sounds an...

... Door Pass welcomes her and reports the number of intruders it foiled during her absence.

Password Journal is a **password** -protected plastic box that stores a diary or other personal items. Anyone seeking to open **Password** Journal must say the correct **password** in the proper voice. Like Door Pass, **Password** Journal reports the number of intruders attempting to open it.

Transaction security (Home Shopping Network...uses speaker verification. Callers who are voice-verified successfully are transferred to the interactive voice- **response** product-ordering module. When **verification** fails, the caller is transferred to an operator.

By the end of June 2000, HSN...

...monitor its curfews.

Outlook

Current research and market trends indicate that future applications of voice- **biometrics** will be text-- independent and incorporate other speech-processing and **biometric** technologies. Such applications are already in demand in several markets. For example, health-care, financial ...

... and other industries that handle large numbers of sensitive documents

have begun to incorporate multiple **biometrics** into their security strategies. The use of products for multiple and layered **biometrics** is further supported by declining prices on **biometric** sensors and development of standards, facilitating the development of multibiometric applications. In April 2000, the...

... University of Wales [1] and elsewhere. Other approaches involve integration of speaker verification and other **biometrics** with public key infrastructure encryption and digital certificates for securing e-commerce applications.

Deployment of...

... verification as a way of extending these applications to secured transactions or as replacements for **PIN** -based security. Moving in the other direction, HSN, for example, is converting its touch-tone...

...as news broadcasts.

These trends indicate acceptance of speaker verification and identification and that voice **biometrics** technologies are increasingly viewed as components in larger, more complex solutions.

1Speech-processing researchers prefer...

... applications beyond the abilities of speech-recognition technology. The result is a weak form of **password** or **passcode** security. "Voice recognition," another confusing term, is often used to refer to speech recognition but card, or a token); what you know (such as a **password** or a **PIN**); and who you are (**biometrics**). 3Vendors have begun using the term "challenge-response" to refer to these systems.

4Speaker identification...

... of precision is unfortunate, because the term also refers to the entire class of "voice- **biometrics** ." The resulting ambiguity is another reason I prefer the term "voice **biometrics** " for referring to the class of speaker-identity technologies.

5The BioAPI Consortium was formed in...

... purpose of developing a specification of a standardized API compatible with a wide range of **biometrics** application programs and **biometrics** technologies. Consortium members now also include **biometrics** vendors and consultants (Identicator, IriScan, ITT Industries, J. Markowitz Consultants, Keyware, Mytec, National **Biometric** Test Center, and Visionics) and **biometrics** users (Barclays Bank, Intel, Kaiser Permanente, U.S. National Institute of Standards in Technology, and...

DESCRIPTORS: **Biometrics ;**

11/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02032618 54563062
Elements of a comprehensive security solution
Katz, David
Health Management Technology v21n6 PP: 12-16 Jun 2000
ISSN: 1074-4770 JRNL CODE: CIH
WORD COUNT: 2427

...ABSTRACT: that determine who is authorized for what access to which information. 3. Employ a strong **user authentication** system. 4. Deny malicious or destructive access to any information asset. 5. Protect data from...
...TEXT: policies that determine who is authorized for what access to which information.

* Employ a strong **user authentication** system.

* Deny malicious or destructive access to any information asset.

* Protect data from end to...

... by a brute-force attack such as the use of a computer program that guesses **passwords** . This is an attack on the ownership of information and intellectual property.

* Corruption of data...

...arise at any of these locations (Figure 1):

* The people who use the system (divulging **passwords** , losing token cards, etc.)

* Internal network connections such as routers and switches.
* Interconnection points such...

... the benefits of networked data communications must contain these elements:

* Physical protection-where are you?

* **User authentication** -who are you?

* Access control-what asset are you allowed to use?

* Encryption-what information...

...not on disks. Disks can be duplicated; smart cards are more difficult to copy.

* Keep **passwords** secure. Avoid writing **passwords** down, then sending them through electronic mail or placing them in messages that are archived ...

...These devices must be locked away or bolted to the desk to guard against theft.
User Authentication

Proof of identity is an essential component of any security system. It's the only way to differentiate authorized users from intruders. **User authentication** to the network is vital for any enterprise that is serious about protecting information assets...

...following elements:

* What the user has or possesses (smart card, certificate).

* What the user knows (**password**).

* A physical attribute (fingerprint or other **biometric** information).

Authentication is most often achieved through **challenge** and response, digital certificates, or message digests and digital signatures.

* **Challenge** and **response** . In this **authentication** method, a software agent within a database system or a workgroup server presents the person resource with a challenge, most often a request for a username and **password** . This is the most common form of security and one that is easily broken when **passwords** are not carefully chosen and maintained. Intrusion Detection Systems (IDS) guard against unauthorized access to...

... uses authentication requires some central authority to verify those identities, whether it be the /etc/ **password** file on a UNIX host, a Windows NT domain controller, or a Novell Directory Services...

11/3,K/3 (Item 3 from file: 15)

02023018 53658041
Biometrics **suites earn a thumbs up**
Bracco, Tere
Network World v17n19 PP: 135-138 May 8, 2000
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 2967

Biometrics **suites earn a thumbs up**

ABSTRACT: The following **biometric** authentication systems are reviewed: 1. BioNetrix Systems' BioNetrix Authentication Suite, 2. Identicator Technology/Identix' BioLogon 2.0, 3. SafLink's SafLink 2000 Multi-**Biometric** Enterprise Security Suite, 4. Keyware Technologies' **Biometric** NT Logon, and 5. American **Biometric** Co.'s Trinity 2.5 and BioMouse Plus. For its combination of security, durability, documentation...
TEXT: Long the guardian of top-secret installations. **biometric** verification is now ready for the fast-paced world of the enterprise network,

The BioNetrix...

... hero encounters a door that won't open without fingerprint, voice or even retina verification. **Biometrics** equipment that authenticates users based on their unique biological features - works well in the world...

...is it for the more pedestrian environment of the enterprise network? How secure is the **biometric** database? Are the **biometric** devices the systems support reliable? Can you manage them without adding staff and/or overtime ...

... cost-effective? And can the devices survive a fall from a desktop? Most importantly is **biometric** authentication right for your company and your network?

If your company has resolved the tangle of ethical issues surrounding **biometric** authentication and has decided to take the plunge, keep in mind that your **biometric** system can't be implemented in isolation from other network systems. Developing and managing a **biometric** authentication system has to be an integral part of your network's total security plan.

Biometric authentication can be extremely secure because it authenticates biological characteristics that are unique to each person.There can be no

stealing, guessing or spoofing of the human **iris** , for example. Furthermore, it is much more secure than a **password** or a token because the former can be guessed, and both can be stolen.

A solid and comprehensive **biometric** authentication system can't be implemented on the fly These systems are complex and, for...

... ask yourself is, "Do I have the time, money and expertise to craft a bulletproof **biometric** authentication system?" Only if the answer is an unequivocal "yes" should you begin to evaluate...

... intent to implement a near-impregnable system, we set out to determine whether network-based **biometric** authentication was ready for the thrills and chills of a large organization. We reviewed only those enterprise-level **biometric** authentication suites designed for network deployment.That means the systems we tested had to do...
... mainly into two groups.The first group, authentication systems based on a combination of fingerprint, **password** and smart card verification, included American **Biometric** Company's Trinity 2.5 (although the company says Trinity will have multiple **biometrics** in future releases and Identix's BioLogon 2.0.

The second group, authentication suites, included BioNetrix Systems' BioNetrix Authentication Suite, Keyware Technologies' **Biometric** NT Logon (an OEM product) and Safi.ink's SafT.ink 2000 MultiBiometric Enterprise Security Suite.

These suites include multiple **biometrics** systems, fingerprint, voice and face verification.The vendors also included a variety of fingerprint scanners...

... database is weak.Therefore, security of the authentication system was our prime concern. In the **biometric** authentication systems we tested, security is handled in one of two ways.

In the first...

... is accomplished via tight integration with NT, in which the authentication system creates fields for **biometric** data storage as extensions to the NT Security Account Manager (SAM) database. These systems take...

... database and provides its own security for this database. BioNetrixAuthentication Suite,Trinity 2.5 and **Biometric** NT Logon employ this means of database security

All the products scored well in self...

... NT Dynamic Link Library (DULL) that challenges users to supply their user IDs, domains and **passwords** . BioNetrix Authentication Suite keeps the GINA level, then adds a **biometric** challenge layer, which means that the product can respond to **authentication challenges** beyond the GINA level.

Further bulletproof ing its security, the BioNetrix product performs client/server...

... story, page 138). All the products we tested let network managers control the type of **biometric** information gathered as well as its relative importance in determining whether system access is granted. For example, SafLink 2000, **Biometric** NT Logon and BioNetrix Authentication Suite all support multiple **biometric** measurements, and the number and type of **biometric** authentications required can be configured for each

individual client workstation.

Trinity 2.5 and BioLogon 2.0 allow network managers to set access parameters based on any combination of **password** , fingerprint or smart card. Again,American **Biometrics** said future releases of Trinity would have more types of **biometric** authentication, but for the time being the only **biometric** support is fingerprint.

In addition, SafLink 2000 also supports smart cards, while BioNetrix Authentication Suite does not. Although Keyware's **Biometric** NT Logon does not support smart cards out of the box, it has a smart...

... also want to sing the praises of the weighted BioDecision Module function of Keyware's **Biometric** NT Logon. Keyware is unique in offering network managers the capability to make access decisions...

... This lets net managers set parameters for allowing anything from full access to retries on **password** entry.

Managing the mysterious
While ease of installation varied little from product to product, manageability...

... BioNetrix product has the slickest installation of any of the products we reviewed.The BioNetrix **Biometric** Starter Kit comes in a neatly packed, clear plastic briefcase that contains everything you need...

...But don't fret about SQL database security because the BioNetrix product stores the database **password** in a secure portion of the NT registry after encrypting it.

We also want to...

... used by the Key ware and Identix products - which also comes packed in BioNetrix's **Biometric** Starter Kit - is far more solid.

The double-dongle construction of the BioMouse Plus from American **Biometrics** may not stand up to normal desktop warfare.

The BioNetrix product, on the other hand, supports nearly every brand of **biometric** authentication device imaginable, giving you the opportunity to select the best breed of each type...
... off to build your biofortress, we want to emphasize that developing and implementing a thorough **biometric** authentication system is a job for professionals, and you will need additional development help to...

...of our technical support calls to Keyware to be returned.

Safety in numbers

All the **biometric** authentication systems we reviewed worked surprisingly well.The fingerprint/ **password** / smart card combinations - Trinity 2.5 and BioLogon 2.0 - are secure and reliable, although Trinity is rather complex and at times overwhelming. Saflink 2000, BioNetrix Authentication Suite and **Biometric** NT Logon are all great choices for shops that need multiple **biometric** authentications. However, for security, flexible manageability and unparalleled support, BioNetrix Systems' BioNetrix Authentication Suite is truly outstanding. Now your mission is to implement **biometric** authentication before your network self-destructs.

OUR 'NOT SO IMPOSSIBLE' MISSION

You can't easily...
... spy, detective and criminal in the course of a review. But with the variety of **iris** scanners, fingerprint readers and voice recognition software we received from the authentication suites, we couldn...90%, there was no sneaking past it.

FaceGuardian, the face recognition application of Keyware's **Biometric** NT Logon, fared somewhat better at a lower sensitivity level of around 80%.

However, the...

... two points that network managers should remember. First, far the most accurate recognition, voice recognition **password** phrases should contain a lot of strong vowel sounds. Second, beware the curse of laryngitis.

Finally, we took a walk on the wild side by testing **iris** scanning, a new and very cutting-edge **biometric** authentication method. **Iris** scanning works on the principle that no two irises are alike in their details, even between identical twins. The human **iris** is as unique as the human retina and a whole lot easier to scan. BioNetrix sent us a copy of IriScan from IriScan, Inc. We borrowed PC **Iris** system-the requisite **iris** scanning hardware - and played with it a bit. Although installation was fairly complicated, once it...
... considering the cost in money and complexity, as well as the eerie "spook hype factor," **iris** scanning seems like overkill for all but the most sensitive of nuclear missile installations.

- Tere...

...PROS: Very good database security; excellent integration with Windows NT CONS: Doesn't support multiple **biometrics** .

SafLink 2000 Multi-Biometic Enterprise Security Suite

RATING:865 COMPANY-SafLink (425) 881-6766; www...

... security; excellent integration with Windows NI CONS: Mediocre auditing and reporting; somewhat complicated installation procedure.

Biometric NT Logon

RATING: 9.05 COMPANY: Keyware Technologies (781) 933-1331; www.keyware.com. COST $89 per user.

PROS: Excellent reliability of **biometric** authentication; unique "weighted decision" module. CONS: Poor documentation; sluggish technical support.

Trinity 2.5 and BioMouse Plus

RATING: 8.25 COMPANY. American **Biometric** Company (888) 246-6687; www.biomouse.com- COST. Trinity client, $49 per seat Trinity Enterprise...

... per server. PROS: Very knowledgeable technical support. CONS: Difficult installation routine; doesn't support multiple **biometrics** (but announced in future versions).

How we did it

We had a blast trying to...

... the security of the authentication database, we evaluated access security as well as encryption for **passwords** and client/server

communications. We then evaluated the ease and security with which these systems...

...provided multiple layers of authentication received higher marks, as did systems that allowed individually configurable **user authentication** levels.

While ease of installation, manageability and database security were our primary concerns, we also...

...prone covers and the like.

SCAN ME

Twelve questions to ask before you deploy a **biometrics** authentication suite.

See a network topology for the BioLogon Server.

White paper on **biometrics** and smart card **user authentication** (PDF format,

Adobe Acrobat reader needed). Read about the challenges that face the **biometrics** industry.

Bracco is also a member of the Network World Test Alliance, a cooperative of...
COMPANY NAMES:
...American **Biometric** Co...

...DESCRIPTORS: **Biometrics** ;

11/3,K/4 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02004506 52027680
Authentication
Kay, Russell
Computerworld v34n13 PP: 77 Mar 27, 2000
ISSN: 0010-4841 JRNL CODE: COW
WORD COUNT: 1129

ABSTRACT: Authentication is the process through which the identity of a computer or network **user** is **verified** ; it is the system that ensures that an individual is, in fact, who he claims...

... can be used to authenticate an individual: 1. something the user knows, such as a **password** ; 2. something the user has, such as a magnetic-stripe card; or 3. something the...
TEXT: DEFINITION

Authentication is the process through which the identity of a computer or network **user** is **verified** ; it's the system that ensures that an individual is, in fact, who he claims...

... access a computer system, network or other protected resource. We think this is what a **password** system does, but **passwords** are only one part of an effective security system. That security system requires three separate ...

... offers little protection to the system. Therefore, the system also usually prompts you for a **password** , a form of authentication.

Authentication

The question, "How do I know you're who you...

... is incomplete and no authorization can or should take place. But how does a system **verify** that a **user** is who he says he is? Simply entering your **password** doesn't prove it's you. Someone else could know your **password** .
The answer lies in a strong authentication process. Basically, the following three factors can be used to authenticate an individual:

1. Something the user knows. This is a reusable **password** , passphrase, **personal identification number** or a fact likely to be known only to the user, such as his mother...

... smart card or a specialized authentication device (called a token) that generates a one-time **password** or a specific response to a challenge presented by the server.

3. Something the user is. This depends on some inherent physical trait or characteristic. Often called **biometrics** , examples of this form of authentication include: fingerprints, retinal (**eye**) patterns, hand geometry, voice recognition, facial recognition, typing pattern recognition and signature dynamics (speed and pressure, not just the outline).

For more on **biometrics** , see "Give Your Computer the Finger" on page 78.

These authentication factors are listed here...

...offers some security. However, each has its own problems or weaknesses. Anyone can enter a **password** and, historically, reusable **passwords** have been vulnerable to guessing, brute force and dictionary-based attacks.

The second means of **authentication** - something the **user** has - requires the user to possess an often difficult-toreplicate device. However this stronger protection...

...in case a device is left at home, lost or stolen.

The third type of **authentication** - something the **user** is is the most difficult to defeat, but it has other problems. **Biometric** identification methods are subject to two types of errors: false positives and false negatives. The...

... no way to give an individual a new identifying characteristic. You can issue a new **password** or security token, but you can't change his fingerprints or **eye** pattern.

Two-Factor Authentication

For greatly increased security, the approach preferred by experts is to...
... two-factor authentication. For example, to use a security token that generates a one-time **password** , you may need to enter a **personal identification number** into the token itself. Similarly, a cardkey can be used in combination with a **biometric** system.

This is essentially what happens when you check in at an airport ticket counter...

...photo ID of some kind. This is something you have with you, and it's **biometric** (something you are) in that the clerk has to determine that the photo on the...

... at that particular time. Some tokens don't show a number continuously but require the **user**

Authentication via Security Token

A hardware authentication device, or security token, provides greatly increased protection against...Some tokens don't show a number continuosly but require the user to enter a **PIN** on the card itself before the number is displayed, thus providing two--factor **authentication** .
ChallengeResponse Systems

With a token-based ChallengeResponse system, the system displays a number (the challenge) when...

... the challenge, then compares its result to the user's response. If they match, the **user** is **authenticated** .

11/3,K/5 (Item 5 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01880150 05-31142
New spec will help secure LANs
Karimi, Hamid; Jain, Vipin
Network World v16n35 PP: 47 Aug 30, 1999
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 638

...TEXT: the enterprise, the call is diverted to a RADIUS server, the server fires off a **password** challenge and, if it receives the correct response, it lets the user into the LAN...

...typically called on to establish peer-to-peer links.

A PPP option also allows for **user authentication** via either **Password Authentication** Protocol (PAP) or **Challenge** Handshake **Authentication** Protocol (CHAP), either of which consults with a company's central Remote **Authentication** Dial-In **User** Service server to validate employee **passwords** .

One of the key features of PPP is its extensibility, and one of PPP's...
... by sending an Access Challenge message back to the switch, effectively asking to see the **password** for that user ID. The switch encapsulates this within EAPOE and sends it to the requesting PC.

The PC then enters its **password** and sends it via EAPOE back to the switch. Typically, **passwords** are sent in encrypted format - compatibility with encryption software is another feature of EAP and...

...protocol for transmission to the RADIUS server.

Once the RADIUS server finds the user ID/ **password** match in its database, it sends a final "success" message to the switch, which now...

... with virtually any current or future security method, including MD5 challenge, token cards or even **biometrics** .

An IEEE working group will soon be assigned to EAPOE.Vendors backing the specification include...

11/3,K/6 (Item 6 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01878226 05-29218
New spec plugs LAN security gap
Duffy, Jim; Fontana, John
Network World v16n34 PP: 1, 76 Aug 23, 1999
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 682

...ABSTRACT: Over Ethernet is intended to keep users from improperly accessing confidential network resources or stealing **passwords** . The proposal defines how to authenticate users on LANs inside a company's firewall.
...TEXT: Ethernet (EAPOE) is intended to keep users from improperly accessing confidential network resources or stealing **passwords** . 3Com, Cabletron, Extreme Networks, FORE Systems, Hewlett-Packard and Intel are among those pitching EAPOE...

... and admit users dialing in to corporate networks from remote sites. PPP usually employs the **Password Authentication** Protocol (PAP) or **Challenge** Handshake **Authentication** Protocol (CHAP) to communicate with Remote **Authentication** Dial-In **User** Service (RADIUS) servers to validate users. (To learn about Diameter, a proposed authentication service that...
... a variety of mechanisms beyond PAP and CHAP including smart cards, Kerberos and one-time **passwords** .

APIs in the works

Microsoft also will supply a set of EAP APIs in Windows...

... servers. The API can be used by third parties to incorporate such authentication mechanisms as **biometrics** or retinal scans into Windows 2000, Cully says.

If those Windows 2000 desktops are attached...

...the Windows 2000 desktop system to validate the user. The desktop system would send the **user** profile to the **authentication** server, and the **user** would gain access to the switch port- and the target server- once the profile was...

11/3,K/7 (Item 7 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01794130 04-45121
Firewall services: More bark than bite
Makris, Joanna
Data Communications v28n3 PP: 36-50 Mar 1999
ISSN: 0363-6399 JRNL CODE: DCM
WORD COUNT: 4647

...TEXT: they're getting the best deal, we've devised a worksheet they can use to **pin** down the precise costs and the payback period (see "Defense Spending").

(Photograph Omitted)

Captioned as... offs in speed and manageability. "People tend to choose proxy firewalls because they have better **user** -level **authentication** and logging abilities," says Eric Novak, product manager for managed security services at MCI Worldcom... to be kept secret. Six carriers say they ask customers to verify themselves via a **password** or by answering a set of predetermined questions when they call the help desk: AT...

...AT&T, Concentric, GTE, Pilot, and PSInet confirm changes by e-mail. Digex customers use **password** -protected voice mail. US West requires customers to send a fax, which is validated by **password** . Concentric and Sprint are the most cautious-they require that specified users authorize changes via...

... Concentric allow customers to make minimal changes (such as adding or deleting users) via a **password** -protected Internet link.

Regardless of the method, find out how accommodating the provider is. Most ... the bells and whistles. Consider support for remote staff: Generally, a smart card and a **password** or digital cer

tificate are needed for authenticating these workers. All providers but AT&T...

... security logs on request, so that customers can get a closer look at events and **verify** **response** time.

When it comes to auditing the network for potential holes, every provider but US...firewalls.

Sidebar:
4. Find out who has access to the firewall. Specify that access is **password** -protected; that way, it will be limited to a few firewall technicians rather than every...

... the trends. Have providers manually look at security logs on a daily basis. A technical **eye** can spot repeated low-level events that intrusion detection tools cannot.

Sidebar:

6. Be a...

...patterns.

Sidebar:

Crack (ftp://info.cert org/pub/tools/crack) Guesswork can be good: This **password** -guessing program locates insecurities in Unix **password** files and notifies net managers of weak log-in codes.

Sidebar:
ISS (Internet Security Scanner...

...on network topology, services, and types of hardware and software.

Sidebar:

COPS (Computer Oracle and **Password** System; ftp://info.cert.org/pub/tools/cops) A collection of programs that identifies security...

...promiscuous mode, a signal that someone is monitoring the network in the hopes of stealing **passwords** .

Author Affiliation:

JOANNA MAKRIS is WAN services editor for Data Communications. She is based in...

11/3,K/8 (Item 8 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01655558 03-06548
Sign on here
Davis, Beth
Informationweek n688 PP: 54-60 Jun 22, 1998
ISSN: 8750-6874 JRNL CODE: IWK
WORD COUNT: 2004

...ABSTRACT: object interceptor, in which the targeted system presents its request for a user ID and **password** via a set of user interface components. The single sign-on system stores those data in an object identifier, plus the associated user ID and **password** . When the object identifier is invoked by a user attempting to log on, the **user** is **authenticated** and then the relevant **password** is plugged in to open a session. A major upgrade is being developed for IBM...

... 1998. The new release will support alternative authentication methods such as fingerprint readers and other **biometric** mechanisms, as well as smart cards. Other single sign-on products that have hit the...
...TEXT: workers access everything from E-mail to high-end production applications using one ID and **password** .

The benefits of single sign-on systems extend beyond enduser convenience. They can boost worker...

...logons.

As client-server applications have proliferated, so have the number of user IDs and **passwords** needed to access them. Character lengths vary, and different systems and applications carry different **password** -expiration processes. One result is that users often write down their many IDs and **passwords** and stick them on their computer monitors-despite business IT security policies that forbid this...

... the sector to achieve rapid growth, despite widespread recognition of the 'too many IDs and **passwords** ' problem," Gartner analyst Helen Flynn says in her report.

(Illustration Omitted)

Vendors seeking to convince... object interceptor, in which the targeted system presents its request for a user ID and **password** via a set of user interface components. The single sign-on system stores that data in an object identifier, plus the associated user ID and **password** . When the object identifier is invoked by a user attempting to log on, the **user** is **authenticated** and then the relevant **password** is plugged in to open a session. With these types of systems, IT departments don...

...link single sign-on systems with back-end systems and applications.

The addition of standard **authentication** methods such as the **Challenge** Handshake **Authentication** Protocol and others means better interoperability among the various systems. Also, most current single sign ...

...summer. The next release will support alternative authentication methods such as fingerprint readers and other **biometric** mechanisms as well as smart cards. IBM also plans to support SAP and other enterprise...

... to move beyond single sign-on to become a provider of systems that also cover **password** synchronization, security, and information access.

Others are also marketing their single sign-on software as...
...controls on a number of systems and applications, as well as synchronize user IDs and **passwords** . Control-SA doesn't reduce the number of **passwords** , but it does help an IT organization centrally manage everyone's **passwords** and access mechanisms.

Information Repository

Here's how it works: Agents are installed on the...

... to manage. These agents gather information from the system and populate a repository with the **passwords** and user IDs that are authorized to the system. For example, an NT system knows which user IDs and **passwords** are allowed to access it, and it keeps that information in a secure user database...

... from any location. Control-SA also lets IT shops sync up the various end-user **passwords** .

Unlike native access, in which a user logs on directly to the application or system, **password** synchronization requires the end user to log on to a subsystem, such as ControlSA, which then matches that user's logon and **password** information, which is held in the repository, with all the various back-end systems the user has authority to access. "With **password** synchronization, when a **password** is changed, Control-SA will change all the other **passwords** ," Shannon says.

Companies with successful single sign-on implementations say the payback is substantial in...

... by Forrester Research Inc. suggests that as much as 80% of help-desk calls are **password** -related. Single sign-on systems could enable a company

...DESCRIPTORS: **Biometrics**

11/3,K/9 (Item 9 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01418007 00-68994
Remote access servers bulldoze road blocks
Borg, Kim
Computer Technology Review v17n4 PP: 1, 6+ Apr 1997
ISSN: 0278-9647 JRNL CODE: CTN
WORD COUNT: 2669

TEXT: Headnote:

Resellers **eye** clear road ahead

In the good old days, the only road blocks remote users had...

... security features when implementing a remote access solution. Security features range from user name and **password** security at the most basic level to activity loggers and call tracking methods (where the device keeps a log containing information such as number of calls received, number of **password** attempts, etc. This allows the network admin to gauge both network security and efficiency); and... via an Ethernet controller. NetRider also employs strong security measures with its point-to-point **Challenge** Handshake **Authentication** Protocol (CHAP) which effectively reduces the possibility of network eavesdroppers stealing **passwords** .

The NetRider 90 system uses a DECserver 90M as its access server component (supporting 57...

... taken care of with BaySecure, a remote access security package that includes dial back, multilevel **password** protection and **user authentication** . For ISDN users, Calling Line Identification provides verification that incoming calls have authorization to connect...access for authorized users but send potential intruders packing, including: automatic dial-back, multi-level **password** protection, **user authentication** audit trails, Point-to-Point Protocol (PPP), **Password** Authentication Protocol (PAP) and CHAP security, Windows NT Domain security, and support for third party...

... concentration of WAN access ports. The 5000 also integrates security with built-in user name, **password** , and callback features. Currently, the 5000 supports standard analog telephone and T1 lines and is...

11/3,K/10 (Item 10 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01296697 99-46093
Gotcha!
Kobielus, James
Network World v13n37 PP: 46-53 Sep 9, 1996
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 1411

...ABSTRACT: requests, files, messages, packets, software modules and network nodes. There are 2 broad product categories: **user authentication** offerings that primarily deliver single sign-on (SSO) access to network resources, and object authentication...
...TEXT: ubiquitous spoofing in which the authenticity of anybody or anything cannot be taken for granted.

Password protection alone is not up to the challenge of securing network access. Hackers can guess or intercept plain-text **passwords** and pass themselves off as authorized users. Electronic messages and files can be modified by...

...third parties before they reach their intended recipients.

To get safeguards above and beyond mere **passwords** , you need a network authentication product. The dozens of such products available today enable you...

...architecture, they all rely on a logon procedure involving at

least two

authentication factors -- a **password** plus something else such as a secure. token, challenge-and-response dialogue, smart card and reader, **biometrics** , digital signature, or public- or private-key cryptography. There are two broad product categories: **user authentication** offerings that primarily deliver single sign-on (SSO) access to network resources, and object authentication...

... you the code needed to add authentication services to existing clients and servers.

An authentic **user**

User authentication products utilize hardware- or software-based tokens to respond to cryptographic **challenges** issued from **authentication** servers. When you initiate a network logon with your user identification and **password** , you receive a numeric string.

If you have a handheld hard

ware token device, you type in that string and your **personal identification number** (**PIN**). The token uses a secret algo

rithm and key produce what is essentially a onetime, nonrepeatable session **password** , and then displays it on an LCD screen. You enter that session **password** on your computer, and if it matches the authentication server's expectation you're granted...

... SecurID, you enter your user ID and Sercurity Dynamics' ACE/Server prompts you for a **password** . In turn, you enter your **PIN** plus the current access code displayed on the token's LCD. The server keeps track...

... they work in the background and make it unnecessary to enter anything more than a **password** or **PIN** . The software token responds to messages from the authentication server.

The vendors with the broadest...

...a computer.

High-tech though they may be, tokens are only as secure as the **passwords** or PINs that users must enter into them. Yet, when implemented and used correctly, tokens...

...resource in question is the proverbial Real McCoy.

To get really secure, you should use **biometrics** such as fingerprint, voice or face recognition: These factors are difficult to steal or copy. A good use for **biometrics** is for securing access to resources that only a few authorized people are allowed to...

... example. Mytec Technologies, Inc. and Secure Computing Corp. are among the vendors supporting third-party **biometrics** products.

The exchange of token and **biometrics** information between server and client is handled by SSO standards such as Remote **Authentication** Dial-In **User** Service (RADIUS), Terminal Access Control Access Control System (TACACS) and Kerberos.

You should look into...

... the gateway or network entry point. The authentication server maintains a database of user IDs, **passwords** , PINs and private keys, which it uses to grant or deny network access.

Compatibility with...

11/3,K/11 (Item 11 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01271601 99-20997
Proposed IETF standard to ease a variety of remote access concerns
Sekar, Richard
Network World v13n33 PP: 31 Aug 12, 1996
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 772

ABSTRACT: A proposed Internet Engineering Task Force standard for administering and securing remote access, called Remote **Authentication** Dial-In **user** Service (RADIUS), would provide a centralized and secure method for authenticating remote dial-in users...

... in to gain access to network resources, the client passes the user's identification and **password** information to the server. Remote users dialing in over digital circuits can change the bandwidth...
...TEXT: connectivity for a number of distant sites radiating out from central headquarters are keeping their **eye** on development of a proposed Internet Engineering Task Force standard for administering and securing remote access.

The scheme, called Remote **Authentication** Dial-In **User** Service (RADIUS), provides a centralized and secure method for authenticating remote dial-in users, authorizing...

... and digital dial-in users. Analog techniques provide a one-to-one relationship between the **user** being **authenticated** and the number of open circuits into the network.

Additional security needs to be enforced...

... in to gain access to network resources, the client passes the user's identification and **password** information to the server.

If the name and **password** correspond to the database information, the server **authenticates** the **user** for the session and grants access to the network resources authorized by the user's...
... As more B channels are dynamically added, the NAS can be configured to require a **password** from the user or a secret key from the end-user device.

Administrators can secure these circuits via static, dynamic or cached **passwords** .

With the first option, before a new circuit is dialed, RADIUS prompts the user to enter a static, reusable **password** . The **password** can be the same one used initially or a different one, as specified in the user profile.

To prevent intruders from capturing the **password** as it is transmitted across the network, administrators can configure the NAS to use the **Challenge** Handshake **Authentication** Protocol (CHAP), a PPP-based

security standard that uses encryption to protect **password** privacyandverifies the identity of a peer. An agreement between the NAS and the end-user station initiates the CHAP procedure.

Alternatively, users can take advantage of dynamic **password** generators, also known as token ID or smart cards, to generate a onetime-use **password** for each additional circuit in the dial-up session when prompted. In this case, RADIUS...
...authentication process.

As a final option, administrators can configure RADIUS to capture a dynamically generated **password** during session initiation for automatic reuse when new circuits are added.

In this case, both the end-user station and the NAS cache the **password** . Then, when dynamic bandwidth is needed, the enduser station provides the CHAPencrypted **password** automatically, and the NAS uses an internal key to authenticate the extra bandwidth transparently. The security administrator can add a timeout value to the cached **password** , or can configure the system to maintain the validity of the **password** throughout the dial-in session.

RADIUS has been available as downloadable software from vendor File...

11/3,K/12 (Item 12 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01220847 98-70242
Glossary
Anonymous
Forbes ASAP Supplement PP: 78 Jun 3, 1996
ISSN: 0015-6914 JRNL CODE: FBR
WORD COUNT: 611

...TEXT: activities that allows activities to be reconstructed.

Authentication: Determining the identity of a communicating party.

Biometric Device: **Authenticates** a **user** by measuring some hard-to-forge physical characteristic, such as a fingerprint or retinal scan...

...into a telephone system to make calls that bypass billing procedures.

Brute Force Attack: Hurling **passwords** at a system until it cracks.

Challenge -Response: A type of **authentication** in which a **user** must respond correctly to a challenge, usually a secret key code, to gain access.

Computer...

... collect a certain number of bytes from the beginning of each session, usually where the **password** is typed unencrypted.

Social Engineering: Gaining privileged information about a computer system (such as a **password**) by skillful lying--usually over a telephone. Often done by impersonating an authorized user.

Spoofing...

... A program that tries a set of sequentially changing numbers (i.e., telephone numbers or **passwords**) to determine which ones respond positively.

11/3,K/13 (Item 13 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01178545 98-27940
Resellers reaping benefits from growth in LAN security
Piven, Joshua
Computer Technology Review v16n2 PP: 1, 14+ Feb 1996
ISSN: 0278-9647 JRNL CODE: CTN
WORD COUNT: 2940

...ABSTRACT: from accessing the network's data. This is typically handled through the use of individual **passwords** and user IDs; a user without a **password** should, in theory, be unable to log on to the network. Unfortunately, this system is...
...TEXT: protect networks. The first is unauthorized access; netadmins must make sure that logon procedures and **passwords** are secure and cannot be duplicated, cracked, or circumvented by unknown and/or unauthorized users ...

... full LAN connectivity while at the same time knowing their connections are secure from prying **eyes** . Similarly, unauthorized users should not be able to dial up a LAN and access data...

...from accessing the network's data. This is typically handled through the use of individual **passwords** and user IDs; a user without a **password** should, in theory, be unable to log on to the network. Unfortunately, this system is...

... a tendency to write down their logon information, thus making it easily available to prying **eyes** and hands. Additionally, a hacker with even a basic knowledge of programming can often bypass...

... FSA Corporation (Calgary, Alberta, CANADA) has announced PowerLogin, a new system for designing login and **password** policies for an entire UNIX network, and managing them from a central location. With PowerLogin...
... can log in when, how, and from where. PowerLogin enables the implementation of fully flexible **password** aging, as well as the creation and management of a central audit trail of logins and **password** transactions. This makes it easy to determine when and where LAN security was breached.

Using PowerLogin's login policy language, system administrators can design login and **password** policies that operate at the user. group, department, or host level to specify criteria such...

... allowed to log in over particular modem lines or over the network, whether any additional **passwords** or other authentication mechanisms are required, etc. PowerLogin includes a controllable **password** -aging system that is fully compatible with NIS, NIS+, and shadow **passwords** .

PowerLogin creates and maintains a centralized logging system for tracking all login and **password** activity, and allows the creation of complex queries to determine the login and **password** transactions that have occurred. PowerLogin can also be used to completely specify the user's...

... centrally managed boot protection feature is available that enables netadmins to control power on/boot **passwords** and eliminate unauthorized access to critical data.

Suggested retail price for Desktop Observatory 4.0...

... often thwarted by the network's own authorized users. These users jot down their various **passwords** and login names on scraps of paper and leave these network "keys" just about anywhere...

... SSO) software to combat this problem. SSO applications are generally script-based and manage multiple **passwords** and logon procedures through a complex authentication process.

CKS (Pittsburgh, PA) has developed another solution...

... sign-on product that uses an authentication server (AS) which acts as a logon "broker," **authenticating** the **user** and processing that user's request for information from the local server (Fig 1). (Fig... LAN protection via a two-factor authentication process. SecurID combines something the user knows: a **personal identification number** (**PIN**), with something the user has: a randomly-generated access code that changes every sixty seconds...
...device with an LED display.

To access a protected network, the user enters his/her **pin** followed by the ID number that appears on the ACE card. The ACE/Server software resides on a TCP/IP network and uses both the **PIN** and the card's **passcode** to identify any user attempting to access a network PC. Without both codes, the user...

... access the LAN. RAC supports PPP (Point to Point Protocol), and through PPP supports the **Password Authentication** Protocol (PAP) and **Challenge** Handshake **Authentication** Protocol (CHAP). RAC also supports tokenized **user authentication** systems, including the aforementioned SecurID. Other security features, including packet, broadcast, and multicast filtering are...

... products are even including dialback security: The user dials in and gives user ID and **password** information; the LAN then dials out to the user, generally at a predetermined phone number...on applications to help secure their networks.

CyberSAFE's Challenger features include kerberized network application, **password** checking, integration with token security cards, and an administrative API that allows applications to modify the principal database. Memco's SeOS offers login filters, **password** controls. Superuser (root) ID protection (a common UNIX weakness), file access control, and host connection...

11/3,K/14 (Item 14 from file: 15)

00957011 96-06404
Safeguard your network
Snyder, Joel
Macworld v12n2 PP: 122-127 Feb 1995
ISSN: 0741-8647 JRNL CODE: MAW
WORD COUNT: 3108

...ABSTRACT: users. The first thing to do is make sure that all dial-in access is **password** protected, and disable guest access to all file servers. IC Engineering has a simple box called the Modem Security Enforcer that makes callers enter a **password** before they get through to equipment. If a new system is being purchased, ignore dialback completely and use a 2-factor system with one-time **passwords** . Options include tokens plus modem interceptors, authentication plus encryption, simpler ARA access, and time-synchronized **passwords** .
...TEXT: mind that network security ranges from low-end issues, like keeping salary figures from prying **eyes** , to the bigger problem of keeping trade secrets from an aggressive competitor. Different solutions exist...

... each is running, which servers offer guest access, and which ones have easy-to-guess **passwords** . This information gives you a better picture of your network, which you can use to...

... Open Collaboration Environment (AOCE), which includes a Key Chain that holds multiple user IDs and **passwords** , all encrypted until unlocked with a single **password** by the end user. (For more about AOCE, see "AOCE--Apple's Plan for Groupware," Macworld, November 1993.) Unfortunately, though, the individual **passwords** are still passed around the network in plain text by many network servers once the...

... a problem. Nevertheless, AOCE's Key Chain can minimize the risk of people writing down **passwords** or leaving them in accessible Preferences documents. (For more about Apple's approach to encryption...servers.

The first thing to do is make sure that all dial-in access is **password** protected, and disable guest access to all file servers. That may sound obvious, but organizations have lost millions of dollars by neglecting to put **passwords** on maintenance ports for routers, switches, and other network equipment--especially voice equipment. If you...

... system. Anyone who dials in to the modem gets connected, but users must enter a **password** before they can actually get through to the device. The MSE is good for small...
... user dials in to a modem, gets connected, and gives a user identification and a **password** . Then the security device hangs up the connection and immediately calls the user back, generally...

...systems into thinking they've made a callback when they really haven't.

One-Time **Passwords**

If you're looking for a new system, ignore dialback completely and use a two-factor system with one-time **passwords** . In a two-factor authentication system, users must provide two different things--for example, a **PIN** (**personal identification number**) and a one-time **password** --to gain access. One-time **passwords** are just that good for one time, one user name. True one-time **passwords** work only once; time-based **passwords** usually expire in 60 seconds or less.

With security based on a one-time **password** , typically you dial in and identify yourself. When the system asks for a **password** , you give the current one-time **password** . The **password** is generated by a calculator-like device called a token, by software on the remote...

... which will fit in the floppy drive of a Macintosh like a disk, to calculate **passwords** , lock the Mac until a **password** is entered, and encrypt data.

In some systems, the token or software calculates the **password** based on a

challenge that the **authentication** system issues. This type of system doesn't just ask for the **password** ; it provides a number (challenge) for the user to enter into the token, which then computes the correct answer (response).

I looked at four approaches to one-time **passwords** for remote access. Each has benefits and drawbacks. One thing is certain, though: two-factor...

... requires authentication before passing a call on to the modem. Optionally, TraqNet dials back an **authenticated user** at a preset number. TraqNet users can use an InfoCard, a token the size of...

... system, an InfoCard user punches two sets of numbers into a touch-tone phone: a **PIN** and the number the token displays. The InfoKey saves the user the trouble of punching in the number--the InfoKey generates the one-time **password** and sends it over the line as soon as the TraqNet system answers. TraqNet is...
...a modem; the GSS resides between the server's serial port and its modem.

This **challenge - response authentication** system uses a calculator-style token, called a WatchWord. The GSS displays a number that the user punches into the WatchWord (along with a **PIN**); the user replies with the number displayed on the GSS. Users must punch in both...

... this language does offer is much greater flexibility in programming and configuration. The company's **authentication** token, which uses **challenge - response** technology, lacks style--it has all the design grace of a 1950s transistor radio.

Digital...

... a completely compatible package called a CryptoCard (prices start at $100 per user).

Time-Synchronized **Passwords** Security Dynamics takes a different approach to authentication. It sells SecurID cards (starting at $58...

... a user whips out a SecurID card and types in the number displayed (plus a **PIN** , of course). No buttons to push, no challenge at all.
The downside of this style... already own. Use the built-in security features of AOCE to reduce the number of **passwords** you have to type each day. Tools like Network Security Guard will help you identify...

11/3,K/15 (Item 15 from file: 15)

00642870 92-57810
Global System for Mobile Communications
Beaudry, Michelle; Parker, Jerry
Telesis n94 PP: 52-69 Jul 1992
ISSN: 0040-2710 JRNL CODE: TLS
WORD COUNT: 9581

...TEXT: style messages, which specify precisely the subscriber's request. This procedure also could include a **password** sequence to ensure security.

DATA SERVICES

GSM also uses the advantages of digital cellular technology...

... telecommunications industry to gain significant experience in how best to achieve such networking.

With an **eye** to the future, BNR has created an architecture for ...The authentication center generates encryption keys and security-related parameters that the MSC uses to **challenge** mobile users to **verify** that they are authorized to use the system. These authentication and encryption control procedures minimize...

... the DMS-HLR (home location register), generates and administers the security-related parameters needed to " **challenge** " mobile subscribers to **verify** that they are authorized to use the system, and to encrypt subscriber data to provide...To counter these threats, the GSM standards specify the following basic security features:

* subscriber confidentiality;

* **personal identification numbers** (PINs);

* encryption of subscriber data, voice, and signaling information; and

* subscriber identity authentication.

To provide...

...GSM network) and are mapped onto IMSIs on the network side.

The second security feature-- **PIN** protection--prevents unauthorized use of a handset if it is stolen. In GSM, the mobile...
...in GSM handsets other than their own.

The SIM itself is protected by an optional **PIN** , which can be altered by the subscriber. If **PIN** protection is enabled, a user must "unlock" the SIM by correctly entering a four-digit number before the handset can be used. The **PIN** , therefore, is used to **authenticate** the **user** to the handset. Once the SIM is active, it uses the internal subscriber-specific authentication...in the handset uses the random number, in conjunction with the stored authentication key and **authentication** algorithm A3, to compute its **response** SRES' (4) to the challenge. The visitor location register checks to ensure that the SRES...

11/3,K/16 (Item 16 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00621996 92-37098
Trusted Products Evaluation
Chokhani, Santosh
Communications of the ACM v35n7 PP: 64-76 Jul 1992
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 6863

...TEXT: etc.). It is the cornerstone for individual accountability.

AUTHENTICATION. This feature allows the TCB to **authenticate** the **user** 's identity. Examples of **authentication** mechanism include **passwords** (6), **biometrics** , **challenge** -response devices (5), etc. In many breakins, we hear that the key weakness has been the ability to compromise the intent of the authentication mechanism by guessing **passwords** . It is very critical to have a protected authentication mechanism that cannot be easily compromised...

...interrupt the login sequence to steal a user (e.g., power on, break key) or **password**). It can be implemented character sequence from the terminal as a request for communications with...D.E. Cryptography and Data Security. Addison-Wesley, Reading, Mass., 1983.
6. Department of Defense. **Password** Management Guidelines. CSC-STD-002-85, April 1985.

7. Department of Defense. Trusted Computer System...

11/3,K/17 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

08300023 Supplier Number: 67372914 (USE FORMAT 7 FOR FULLTEXT)
Fighting fire with fire.(network security and firewalls)
Computer Business Review, v7, n4, p50
April, 1999
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 1627

... product, Access Denied, a security device intended to prevent two modems handshaking until the outside **user** has been properly **authenticated** , stood up to the **challenge** . But one hacker could not stop himself venting his frustration at being kept out.
In...

...the choices are therefore considerably more complex than many firewall vendors suggest.
(GRAPH OMITTED)
WATCHFUL **EYES**
Sitting as a gateway between the Internet and a company's internal network, firewalls can...Instead of having to remember a collection of often forgotten or confusing log-in names, **passwords** and procedures, single sign-on, as the name might imply, means the user only needs...

...decryption keys held on personal smartcards and, if further safeguards are required, the use of **biometric** identification.
In many cases though, the hacker is smart, but not that smart. In one...

11/3,K/18 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

08012824 Supplier Number: 66163578 (USE FORMAT 7 FOR FULLTEXT)
BioNetrix Joins Check Point Software OPSEC Alliance.
PR Newswire, p3521
April 24, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 586

... same time, migrate to more conclusive forms of authentication such as smart cards, tokens and **biometrics** .
"BioNetrix's membership in OPSEC will enable organizations to cost-effectively build secure business processes...

...the Check Point Secure Virtual Network architecture.

"Real world VPN-1 deployments will use multiple **authentication** solutions ranging from **challenge / response** tokens and PKI to **biometric** devices, and hence, our open integration support within OPSEC for authentication technologies," said Bradley Brown...

...their support for the Secure Authentication API (SAA) to further ease the management of end **user authentication** ."

About BioNetrix

BioNetrix is the only security innovator to provide direct personal assurance, conclusively verifying the identity of an end **user** . The BioNetrix **Authentication** Management Infrastructure reduces costs and increases security in all computing environments through the deployment of authentication technologies -- from **passwords** , tokens and smart cards to **biometrics** . Network Computing magazine recently named the BioNetrix Authentication Suite as its "Editor's Choice" (see...

11/3,K/19 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07967302 Supplier Number: 66573361 (USE FORMAT 7 FOR FULLTEXT)
Wearable Java Computer from Dallas Semiconductor has Large, 200 Kbyte Memory for Secure Corporate Log-on and Personal Uses.
Business Wire, p0335
Nov 2, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1441

... public-key certificate format. In addition, the DS1957B can store hundreds of user names and **passwords** , a color ID picture, and the application programs of many different service providers.

All personal...

...time for applications including:

-- Access control to buildings and equipment

-- Secure network log-on using **challenge** /response **authentication**

-- Storage vault for **user** names and **passwords**

-- User profile for rapid Internet form-filling

-- Digital signatures for e-commerce

-- United States Postal...

...Security Device for PC Postage(TM)
downloadable over the Internet

-- Digital ID photo and fingerprint **biometrics**

The iButton can be updated for Web-based applications not yet invented. Because its memory...

...emerges in the marketplace, users will want to get rid of the cumbersome user name/ **password** sign-on methodology wherever possible. A much more secure method of logging onto computers is...log onto a network, sign an electronic document, safely store a list of user names/ **passwords** , keep a copy of an ID photo, and accept updates for the e-commerce transactions...

11/3,K/20 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06930288 Supplier Number: 58538373 (USE FORMAT 7 FOR FULLTEXT)
BioNetrix Authentication Suite Earns Network Computing Editor's Choice Award.
PR Newswire, p0084
Jan 12, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 379

... with an infrastructure to manage existing systems and prepare for new forms of authentication including **biometrics** .
In its reviews of **biometric** authentication management solutions, Network Computing tested authentication systems from four vendors and judged each on...

...It stated that as "the network enterprise continues to be a mix of platforms and **authentication challenges** , the BioNetrix software suite looks to the future, in which your authentication system encompasses several...

...Authentication Management Infrastructure (AMI), a standardized open platform for managing disparate authentication technologies such as **passwords** , tokens and **biometrics** .
"We are extremely pleased in receiving accolades from Network Computing," said Peter Bianco, president and CEO of BioNetrix. "This award further validates our belief that the world is moving towards **biometrics** ."
The review stated that BioNetrix "has set its sights beyond **biometrics** and is working to embrace any and all authentication technologies. As such, the suite goes...

...ease user and policy management, while still offering a relatively high level of security for **user authentication** ."
About BioNetrix
BioNetrix is the only authentication innovator to provide an Authentication Management Infrastructure that...

...and increases security in all computing environments through the deployment of superior authentication technologies -- from **passwords** , tokens and smart cards to fingerprints, facial recognition and voice verification. The company's flagship...

11/3,K/21 (Item 5 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06895461 Supplier Number: 58374360 (USE FORMAT 7 FOR FULLTEXT)
BioNetrix Suite Covers All the Bases -- The vendor takes our Editor's Choice by doing more to simplify user and policy management while keeping a high level of authentication security. (BioNetrix Systems' BioNetrix Authentication Suite 2.0 biometric -based network security software) (Software Review) (Evaluation)
O'Shea, Timothy M.; Lee, Mike
Network Computing, p47
Dec 27, 1999
Language: English Record Type: Fulltext
Article Type: Evaluation

Document Type: Magazine/Journal; Trade
Word Count: 3756

...while keeping a high level of authentication security. (BioNetrix Systems' BioNetrix Authentication Suite 2.0 biometric **-based network security software) (Software Review) (Evaluation)**
... BioNetrix Systems' BioNetrix Authentication Suite 2.0 for Microsoft Windows NT is the most robust **biometric** authentication system in this immature market. The vendor has set its sights beyond **biometrics** and is working to embrace any and all authentication technologies. As such, the suite goes...

...ease user and policy management, while still offering a relatively high level of security for **user authentication** .
BioNetrix supports four devices: American **Biometric** BioMouse, T-Netix VoicEntry, Veritel Corp. Voice, and Visionics Corp. FaceIt. Additionally, the product offers a **password** system that can replace or supplement the NT **password** for extra security. The suite provides a central management system for these devices, as well as for an organization's **user - authentication** needs, even beyond **biometric** technology. At the heart of the system, the program's BioServer software provides for **user authentication** and tackles **user** , group and policy management. BioServer's six modularized data elements (BioUsers, Workstations, BioApplications, BioDevices, BioPolicys and Reports) provide flexibility for controlling users, applications, realms, **biometric** devices, groups and policies.
With its hierarchical directory structure model, BioNetrix makes it easy to set up the right level of security, from a simple **password** to a **biometric** -enabled workstation with several authentication layers. Making changes is a drag-and-drop maneuver.
While...
...hook contacts the BioServer, which opens a path to the client that ships down the **biometric** template and policy.
Installation requires Microsoft's SQL Server as the database back end to store information about users, groups and **biometrics** . We were initially concerned with security related to how the BioNetrix software obtains the SQL Server **password** . The vendor explained that the database **password** is encrypted and stored in a secured section of the NT registry.
BioNetrix Administration Manager...

...data.
The software's six main modules allow for easy user management and construction of **biometric** policy, again via drag-and-drop. It's easily managed, but it will probably take...

...set policies and authenticated against the server. The neatly formatted reports detail authentication usage, failed **authentication** attempts, system **user** information and system users listed by Authentication Client. This information is stored in the database and can be exported and parsed by SQL-aware reporting packages.
BioNetrix's approach to **biometric** authentication and security is well-conceived. Unlike the other products we tested, BioNetrix does not...
...levels of NT authentication. By relying on an initial login to NT before applying a **biometric challenge** layer, BioNetrix won't miss **authentication** requests outside the GINA (Graphical Identification and Authentication) level. This is important; there are several...

...t create vendor-specific solutions to these issues while it still provides a layer of **biometric** security. The one downside to which BioNetrix admits is requiring the user to enter a user name and **password** in addition to providing a **biometric** . However, BioNetrix plans to address these issues in version 3.0, and provide streamlined support end, and has

developed its own user management interface for version 3.0.

BioNetrix **Authentication** Suite, $45 per **user** , BioNetrix Systems Corp., (800) 397-7561, (703) 734-9200. www.bionetrix.com or info@bionetrix ...

...0 Server for Windows

Grade: B-

A rich feature set combined with a well-constructed **biometric** authentication model earned Identicator Technology's BioLogon 2.0 high marks in our tests. We...

...the quality of integration into the existing NT environment.

BioLogon offers eight combinations of fingerprint, **password** and smart-card **authentication** . Using **biometrics** , **user** accounts can be enrolled with multiple fingers per user-four by default and up to...

...Like the products from Saflink and NEC, BioLogon integrates its solution into the existing NT **user** management and **authentication** systems. Identicator makes proprietary extensions to the SAM (Security Account Manager) database, incorporating its own fields for **biometric** storage.

We configured **biometric** policies for new and existing users easily through an intuitive dialog box. For **biometrics** users, BioLogon defaults to allow login with either fingerprint or **password** . If you select a **biometric** -only login, BioLogon offers to generate a new user **password** automatically. By default, the software leaves existing user **passwords** untouched, but BioLogon offers an easily configurable system for **password** management. BioLogon can generate a random **password** , as do the NEC and Saflink products, but it goes a step further in its integration with NT. We were able to configure **password** generation in accordance with NT expiration settings, or set our own triggers based on number...

...click configuration. We chose the self-enrollment option and elected to have our newly created **biometric** logon policy applied after the self-enrollment was completed. A default **biometric** user policy can be configured via a pull-down menu option from the main user...

...and after a scan and verification scan was authenticated into the domain as a new **biometrics** user. Subsequent logins allow one-touch authentication from the login, but nonbiometrics users must enter...

...full diagnostics. We enabled the diagnostics to provide an event-by-event description of the **biometric** authentication activities. The Components tab offered us a diagnostics button to check that all installed...

...remote enrollments: A device attached to the server isn't the only way to create **biometric** users.

Despite these minor flaws, BioLogon was the most capable of the three products that...

...fax (650) 873-8653. www.identicator.com or info@identicator.com.

Saflink Corp. SAF2000 Multi- **Biometric** Enterprise Security Suite

Grade : B-

With the modular SAF2000 Multi- **Biometric** Enterprise Security Suite, Saflink strives to provide interoperability across an authentication environment. It supports authentication...by name. In either mode, authentication comparisons are performed on the server. We chose fingerprint **biometrics** support for our testing. Face and voice **biometrics** are also available and, like the BioNetrix system, multiple **biometrics** may be used based on a client workstation's configuration. Unlike BioNetrix or TouchPass, SAF2000...

...panel handle configuration. Server Manager provides basic functionality to add computers and enable or disable **biometrics** on client workstations. Through the control panel, we could select the location of the SAFserver (for client access), set our **password** generation options and configure auditing. Like the products from NEC and Identicator, Saflink integrates **biometric** enrollment with the existing NT user manager.

While the SAF2000 management system's complexity may...

...streamlined.

We took issue with SAF2000's default action on user enrollment of replacing the **password** with an unknown random. This default setting can be changed, but it could lock out users if there's any problem with the initial **biometric** enrollment. Although **password** replacement has its benefits, we preferred the Identicator model, which allows for configuring the **password** expiration and replacement criteria.

SAF2000's basic but informative event logging tracks **biometric** activity. We could easily see time-stamped entries for each user login, including failed attempts associated with a unique identifier (the SAFtyPIN) generated from the user's unique **biometric** characteristics. But because these auditing features are disabled by default, you need to select them...

...The application will also configure licensing for remote servers within the same domain.

SAF2000 Multi- **Biometric** Enterprise Security Suite, $199.95 including one server license and 10 user licenses, Saflink Corp...

...cleanly with Windows NT on the PDC and with the SAM database for storage of **biometric** user data.

TouchPass aims to be seamless to the desktop user and offers the convenience of a one-to-many lookup for the **biometric** authentication. Just place a finger on the scanner; TouchPass handles the rest, including authorization policy...

...and were disappointed to see that TouchPass added little to the environment besides the basic **biometric** integration with NT's user manager. This integration was limited compared to the additional user management functionality offered by the products from Saflink and Identicator. The **biometric** module for the user manager offers only one set of options, related to the type...

...security of fingerprint accuracy.

We were also perplexed when we tried to enroll an existing **password** -only user as a **biometric** -or- **password** user and TouchPass replied, "You must enter a **password** ." Our user had a legitimate **password** , yet TouchPass couldn't circumvent NT 4.0 security to obtain and store the user **password** . Be prepared to change some **passwords** at enrollment. For each user enrolled, you can randomly generate a **password** via a one-button click.

To TouchPass' credit, the software allows enrollment of up to...

...another fingerprint.

On the client side, we liked TouchPass' automatic fingerprint detection for one-touch **authentication** . Other products require **user** names to be entered in addition to the prints. Early in testing, however, we were...

...problem via a CTRL-ALT-DEL override sequence that let us type in our account **password** . This override works only if the user has a **password** in addition to the **biometric** .

TouchPass does not identify the workstation in configuring clients as other products do. The TouchPass **authentication** model is wholly **user**

-based and relies on the NEC GINA to provide **biometric** authentication between client and server. The TouchPass client design maintains a clever local cache with...

...files of users who recently logged into a workstation. This process lets TouchPass speed the **biometric** verification and authentication procedures. It also has the benefit of enabling the user to log...

...at mlee@nwc.com.
Sidebar: Fingerprint Scanners: Hands On
If you plan to pursue a **biometric** authentication solution, consider the benefits and limitations of the **biometric** device you choose. Fingerprint scanners are our **biometric** device of choice because of their decreasing cost, increasing popularity and continued integration into the ...

...readily identify with the fingerprint scanner and use it on the desktop. There are other **biometric** technologies-voice recognition, retinal scanners, camera-based facial recognition systems and signature recognition, to name a few. But we think fingerprint scanners are a proven favorite in **biometric** authentication, offering the best solution for a variety of needs.
The fingerprint scanner works by...

...environment and needs. Cost is always an important consideration as you determine the number of **biometric** authentication devices you'll need. Remember that each system we tested will let **passwords** be used, and others (Indenticator Technology's BioLogon, for one) provide support for specific smart...

...User Level" (InformationWeek, Sept. 27, 1999) www.iweek.com/754/nec.htm
"Buyer's Guide: **Biometrically** Speaking" (Network Computing, August 23, 1999) www.networkcomputing.com/1017/1017buyers2.html
"Six **Biometric** Devices Point the Finger at Security" (Network Computing, June 1, 1998) www.networkcomputing.com/910...

11/3,K/22 (Item 6 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06895460 Supplier Number: 58374359 (USE FORMAT 7 FOR FULLTEXT)
Biometric **Authentication Management -- Biometric authentication systems are being integrated into desktop systems. We tested four products that help manage the** biometric **data.(BioNetrix Systems' BioNetrix Authentication Suite 2.0, Identication Technology's BioLogon, Saflink's SAF 2000 and an unnamed product from NEC Technologies)(Software Review)(Evaluation)**
O'Shea, Timothy M.; Lee, Mike
Network Computing, p44
Dec 27, 1999
Language: English Record Type: Fulltext
Article Type: Evaluation
Document Type: Magazine/Journal; Trade
Word Count: 1298

(USE FORMAT 7 FOR FULLTEXT)
Biometric **Authentication Management -- Biometric authentication systems are being integrated into desktop systems. We tested four products that help manage the** biometric **data.(BioNetrix Systems' BioNetrix Authentication Suite 2.0, Identication Technology's BioLogon, Saflink's SAF...**

TEXT:
...be better than using these to identify network intruders? By relying on unique biological traits, **biometric** authentication systems have proved their worth for years in standalone applications within high-security environments...

Biometric hardware can provide authentication via voiceprint, facial scan, retinal patterns and fingerprints. With so many options available, vendors have begun developing software to integrate the devices into everyday networks.

Biometrics has moved from simple desktop implementations to network-authentication systems. New applications provide solutions to...

...an overwhelming number of products-330, according to the ICSA (International Computer Security Association) 1999 **Biometrics** Survey-are marketed by a diverse pool of vendors, which raises concerns over standards, integration...

...Promising changes and enhancements to security, the upcoming release of Windows 2000 is also keeping **biometrics** vendors on their toes. Each vendor whose product we tested is scheduling version releases in...

...front, several proposals are in development, most notably HA-API (Human Authentication API) and BAPI (**Biometric** API). HA-API (released in 1997) provides a means to interface to various **biometric** technologies, but only under the Win32 platform. BAPI, under development by the BioAPI Consortium, provides an OS-independent standard and makes the API **biometric** -independent. The first version of this standard is expected in the first quarter of 2000...

...to support other devices on an as-needed basis.

Beyond the lack of firm standards, **biometric** technology still gets a bum rap from end users. Many associate fingerprint scanning with the...

...of our unique biological traits makes some feel their privacy is being violated. Also, though **biometric** authentication can ease administrative headaches, such as **password** management, and improve upon user identification, integrated support across the enterprise is missing. Don't ...

...such features; they're just not here yet.

Nevertheless, it makes no sense to ignore **biometrics** . This developing and dynamic market has drawn vendors who are constructing smart products and simplified...

...to join early adopters from financial institutions, health and pharmaceutical companies and government organizations.

No **biometric** system will let you rip out the existing authentication structure. Most shops maintain a combination of authentication technologies, and your **biometric** solution should offer some appreciation of these systems, or provide a model that will integrate ...

...the future. Products that best accomplish this integrate existing technologies (such as smart cards) with **biometrics** and establish a management interface that allows for the addition of modules to support new technology. Shops that are in good shape for **biometrics** will have a largely homogeneous Windows NT platform with an authentication system that is primarily **password** -based. Larger shops may be able to integrate **biometrics** into specific applications or for some users as the market develops.

Our Editor's Choice...

...Windows 2000 looms and the network enterprise continues to be a mix of platforms and **authentication challenges** , the BioNetrix software suite looks to the future, in which your authentication system encompasses several...

...How We Tested
In selecting products for our tests, we focused on systems that provide **biometric** authentication into a network environment. We rounded up solutions that offer an integrated system for...
...as our platform, primarily because of widespread vendor support for the environment. Fingerprints were our **biometric** of choice because the compatible hardware is accessible, dropping in price and widely supported. Vendors...

...final pool.
We tested each product to determine its ability to provide basic authentication via **biometrics** within a closed network (consisting of an NT server and NT workstation clients). We were particularly interested in the integration of the **biometric** software with the NT authentication systems. As the products were installed and configured, we noted...of RAM, running Windows NT Server 4.0 updated with Service Pack 5.
Executive Summary -- **Biometrics**
Network-level **biometric** authentication-the use of fingerprints, facial features and voice characteristics to identify users-is getting...

...focused our tests on vendors who were offering shipping products and tested only fingerprint-scanning **biometric** devices-these devices are most accessible, lowest in cost and supported by every vendor of...

...client software and at least one fingerprint scanner. We identified the function of the network **authentication** and **user** -management systems being provided by **biometrics** vendors. The performance of the fingerprint devices was beyond the scope of our tests. The...

11/3,K/23 (Item 7 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06615656 Supplier Number: 55677582 (USE FORMAT 7 FOR FULLTEXT)
Security Dynamics Outshines Field.(review of four network security software products)(Software Review)(Evaluation)
O'Shea, Timothy M.
Network Computing, p14
Sept 6, 1999
Language: English Record Type: Fulltext
Article Type: Evaluation
Document Type: Magazine/Journal; Trade
Word Count: 3201

... Editor's Choice
Grade: A-
For many, the name Security Dynamics is synonymous with strong **user - authentication** solutions. Ace/Server version 3.3.1 with SecurID scored highest in our tests, and...

...access.
We chose the client's interactive authentication test before jumping into normal authentication. This **authentication** mode allows a **user** to bypass the challenge if necessary. This can be a lifesaver: If you neglect to...

...authentication. When we configured the server end, we configured our user account to "select own **PIN** ." At the first client authentication we entered a token code and were prompted to select and verify a **PIN** . However, on our next attempt we couldn't get through. After checking network connections and...

...had been locked out by Ace/Server's "Evasion-of-Attack" security after three unsuccessful **passcodes** .

The root of those first three failures was our misunderstanding of SecurID's **PIN** / **passcode** scheme. Where other tokens allow you to key in your **PIN** , the SecurID key fob lacks any input method. You are required to enter your authentication code in the form **PIN** +TOKEN...

...bet your users will too, especially if they get that initial prompt to configure their **PIN** .

It is also important to note that SecurID uses a patented time-synchronization scheme to...

...count on time being in sync on the token and the server so the right **passcodes** are being calculated. Fortunately, an administrator can resynchronize an errant token through the user manager...these points with open-development support and you have a competitive solution in the strong **user authentication** market.

CryptoAdmin 4.0, starts at $5,000, CryptoCard, (800) 514-8809, (613) 599-2441...

...button and bounce ourselves out of the management window.

Users can be imported from Unix **password** files, a comma-separated ASCII file, Unix-based RADIUS **password** lists and from the Shiva LANRover. We threw the university's 30,000-line Unix **password** file at the import routine and watched as VACMan chugged slowly along importing users until... we had specified on the server was kicking in on the client. After entering the **password** and token-generated digits, we were in.

Vasco has numerous tokens ranging from the phaser...

...popular hardware token.

We found this plastic token difficult to hold while keying in our **PIN** and responses. The 300 includes an LED array at its tip for automatic entry of your **authentication challenge** . A clever gimmick, we found no manner of adjustment could make this method any faster...

...bright red color, this device can be used to "unlock" user tokens after the incorrect **PIN** limit has been reached. Keying in the lock code found on the user token will...

...the administrative token. This code unlocks the user's token, which then requests a new **PIN** . We were intrigued by this process, so we threw numerous random numbers at the administrative...

...purposes, we focused on V-One's client/server offerings and how it performed basic **user authentication** .

We were immediately impressed with the number of other tokens and authentication services the V...

...the client. V-One's approach is that it will distance the client from the **user** so that **authentication** and VPN initialization is seamless. Unfortunately, in doing this it has made the client difficult...

...for backbone service, this type of product could represent the future of client/server strong **user authentication** systems as remote access servers fall by the wayside. If your interests are still heavily...the form of a keypad-or none at all. Most input is solely to allow **PIN** entry to

"unlock" the card and let the user see the proper **pass code** . Some cards offer additional authentication schemes or programmability that can be selected through this interface...

...of these additional features change the basic idea behind a token-it is something the **user** holds, **verifying** he or she is authorized to have access.
In choosing a token solution, it is...

...forget to take your token with you.
Web Links
"Vendors Simplify Authentication Using Tokens and **Biometrics** " (InternetWeek, June 3, 1999) www.internetwk.com/story/INW19990603S0007
"Authentication With More Smarts" (InternetWeek, March...

11/3,K/24 (Item 8 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06604340 Supplier Number: 55625348 (USE FORMAT 7 FOR FULLTEXT)
New spec will help secure LANs.(Technology Information)
Jain, Hamid Karimi And Vipin
Network World, p47
August 30, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 632

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...the enterprise, the call is diverted to a RADIUS server, the server fires off a **password** challenge and, if it receives the correct response, it lets the user into the LAN.
... typically called on to establish peer-to-peer links.
A PPP option also allows for **user authentication** via either **Password Authentication** Protocol (PAP) or **Challenge** Handshake **Authentication** Protocol (CHAP), either of which consults with a company's central Remote **Authentication** Dial-In **User** Service server to validate employee **passwords** .
One of the key features of PPP is its extensibility, and one of PPP's ...

...by sending an Access Challenge message back to the switch, effectively asking to see the **password** for that user ID. The switch encapsulates this within EAPOE and sends it to the requesting PC.
The PC then enters its **password** and sends it via EAPOE back to the switch. Typically, **passwords** are sent in encrypted format - compatibility with encryption software is another feature of EAP and...

...protocol for transmission to the RADIUS server.
Once the RADIUS server finds the user ID/ **password** match in its database, it sends a final "success" message to the switch, which now...

...with virtually any current or future security method, including MD5 challenge, token cards or even **biometrics** .
An IEEE working group will soon be assigned to EAPOE. Vendors backing the specification include...

11/3,K/25 (Item 9 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06586692 Supplier Number: 55548263 (USE FORMAT 7 FOR FULLTEXT)
New spec plugs LAN security gap; Vendors get behind Ethernet authentication protocol. (Extensible Authentication Protocol Over Ethernet) (Technology Information)
Fontana, Jim Duffy And John
Network World, p1
August 23, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 669

... Ethernet (EAPOE) is intended to keep users from improperly accessing confidential network resources or stealing **passwords** . 3Com, Cabletron, Extreme Networks, FORE Systems, Hewlett-Packard and Intel are among those pitching EAPOE...

...and admit users dialing in to corporate networks from remote sites. PPP usually employs the **Password Authentication** Protocol (PAP) or **Challenge** Handshake **Authentication** Protocol (CHAP) to communicate with Remote **Authentication** Dial-In **User** Service (RADIUS) servers to validate users. (To learn about Diameter, a proposed authentication service that...
...a variety of mechanisms beyond PAP and CHAP, including smart cards, Kerberos and one-time **passwords** .
APIs in the works
Microsoft also will supply a set of EAP APIs in Windows...

...servers. The API can be used by third parties to incorporate such authentication mechanisms as **biometrics** or retinal scans into Windows 2000, Cully says.
If those Windows 2000 desktops are attached...

...the Windows 2000 desktop system to validate the user. The desktop system would send the **user** profile to the **authentication** server, and the **user** would gain access to the switch port - and the target server - once the profile was...

11/3,K/26 (Item 10 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06225031 Supplier Number: 54234283 (USE FORMAT 7 FOR FULLTEXT)
Keep An Eye **Out For The Hidden Costs. (cost of remote support for virtual private networks users adds up) (includes glossary of VPN acronyms) (Technology Information)**
Salamone, Salvatore
InternetWeek, pV5(1)
March 29, 1999
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 2066

Keep An Eye **Out For The Hidden Costs. (cost of remote support for virtual private networks users adds...**
... up stage for VPN adoption.
--
VPN Acronyms
ATM-asynchronous transfer mode
CA-certificate authority
CHAP- **Challenge** Handshake **Authentication** Protocol

DES-Data Encryption Standard
DHCP-Dynamic Host Configuration Protocol
DNS-Domain Name Service
EDI...Point-to-Point Compression
MPPE-Microsoft Point-to-Point Encryption
NAT-Network Address Translation
PAP- **Password** Authentication Protocol
PKI-Public-Key Infrastructure
POP-Point of Presence
PPP-Point-to-Point Protocol...

...to-Point Tunneling Protocol
PSTN-Public Switched Telephone Network
QoS-Quality of Service
RADIUS-Remote **Authentication** Dial-In **User** Service
SKIP-Simple Key Management for IP
SLA-service level agreement
SSL-Secure Sockets Layer...

11/3,K/27 (Item 11 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05903931 Supplier Number: 53119818 (USE FORMAT 7 FOR FULLTEXT)
REMOTE POSSIBILITIES FOR THE ENTERPRISE.(Company Operations)
Network, p97(1)
July 1, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 3216

... an authentication server. Users log in with a login ID, which generates a unique alphanumeric **password** every 60 seconds. For one more level of security, encrypted tunnels will be developed between...North America, and Asia Pacific.
To access their sites over the Internet, partners have a **password** that is changed frequently. The HP 9000 Unix-based servers have built-in security, but...

...Hamilton.
Through EBF, select customers can tap into a range of specially tailored, for-their **eyes** -only Web pages. The information provided on these pages ranges from a listing of what...
...eligibility.
To access EBF, Hamilton says customers "only need to register once, maintain one secure **password** , and have one hole in their firewall for delivery of services." But there are other...

...is to have multilayers of security--depending on the level of service. Beyond the basic **password** , a user's ability to tap into the main access level of information is restricted...be performed on a variety of external servers, including Lightweight Directory Access Protocol (LDAP), Remote **Authentication** Dial-In **User** Service (RADIUS), Windows NT, Security Dynamics, and Axent. Encryption support includes RC4, DES, and Triple...

...the same security issues regardless of the switch or vendor we used," Brandt explains. "The **challenge** is getting the **authentication** part right, and we haven't fully worked through those issues; this is why we...

11/3,K/28 (Item 12 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

05603307 Supplier Number: 48479324 (USE FORMAT 7 FOR FULLTEXT)
MEMCO Software Announces Single Sign-On Partner Strategy.
Business Wire, p05121280
May 12, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 728

... party authentication mechanisms depending on their security requirements. MEMCO is working closely with the top **authentication** vendors, including CyberSafe (**Challenger**), Entrust (Certificates), NRI (**Biometrics**), SecureComputing (Safeword) and Security Dynamics (SecureID). MEMCO is also developing an Authentication Toolkit to assist...

...with Proxima. This approach will enable Proxima customers to use virtually any mainstream method of **user authentication** .
MEMCO's Encryption Partners
To strengthen network security, MEMCO is working with Entrust's PKI...

...product can be used with Proxima to further secure network transfer of user IDs and **passwords** as well as communication between Proxima SSO and its application agents.
MEMCO's Security Administration...

11/3,K/29 (Item 13 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05571602 Supplier Number: 48436993 (USE FORMAT 7 FOR FULLTEXT)
VASCO Data Security Announces The Arrival Of A Newcomer To The Digipass Family
PR Newswire, p0421CHTU008
April 21, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 989

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...OTC-Bulletin Board: VDSI) introduces the Digipass 300, an extension of its Digipass family of **user authentication** devices, or tokens. Digipass 500 and now Digipass 300 secure remote access and **user authentication** for financial institutions, companies and organizations. Along with Digipass 500, Digipass 300 will become a...
We have chosen the Digipass 300 because it is a modern-looking, **user** - friendly **authentication** device that we could easily integrate in our existing security infrastructure," said Harald Fatland, Project...

...factor authentication. To accesssomeone's system the user needs two things: the Digipass and a **password** or **PIN** code. Without both elements, you cannot gain access to the system or network. The Digipass...

...can arise from human error."

Digipass 300: VASCO's latest innovation for secure access and **user**
authentication

Provides top-level **user** -friendliness
The Digipass 300 represents the newest addition to the Digipass family of low-cost, **password** -protected, personal identification tools. Its high-speed optical interface allows **challenge / response** **authentication** , server **verification** and digital signature. In addition, the token supports all standard, single and triple Data Encryption...

...degree of flexibility for both security integrators and network system managers. Security parameters such as **PIN** length, number of **PIN** trials, number of host computers, type of algorithm, lengths of challenge and response are all...

...strategic objectives. From providing strong authentication technology in the form of tokens, smart cards, and **biometric** technology, to integrated authentication, access control, accounting and auditing, VASCO is at the forefront of...

11/3,K/30 **(Item 14 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)

05318728 Supplier Number: 48096456 (USE FORMAT 7 FOR FULLTEXT)
Unlocking Virtual Private Networks
Fratto, Mike
Network Computing, p52
Nov 1, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 5438

... a VPN between them so that at no point is personnel information exposed to prying **eyes** .
As a conceptual networking model, virtual private networking holds great promise. The trouble is, there...in two areas: remote user dial-up tunneling and LAN-to-LAN tunneling. Encryption and **user** **authentication** relies on Microsoft's Point-to-Point Encryption, which uses the RSA RC4 encryption algorithm...

...encryption algorithms such as DES or BlowFish, you won't be able to employ PPTP. **User** **authentication** is PPP-based with **Challenge** Handshake Access Protocol (CHAP), MS-CHAP and **Password** Authentication Protocol (PAP) available, and it uses NT Domains for its user database to ease **user** and server **authentication** management.
PPTP dial-up tunnels are implemented in two ways, depending on client connectivity. In...and interoperate with other CAs.
Aventail's VPN 2.0 offers much of that strong, **user** -based **authentication** and encryption and **user** -based access, as well as a host of other features that are not possible with...

...encryption and network resource access users have. When users attempt to access protected services, the **user** has to **authenticate** and, if successful, the security profile is enforced and the connection continues.
For example, a...

...be processed as normal. The user profile on VPN 2.0 might state that this **user** needs to be **authenticated** with the MD5 hash algorithm, can access the personnel database and requires DES encryption. When...

...0. VPN 2.0 creates a Secure Sockets Layer (SSL) session with the client and **authenticates** the **user** . Once the **user** is **authenticated** , VPN 2.0 sets up the encrypted session and the **authenticated** **user** can access the

database.
* A Proprietary VPN VTCP/Secure from InfoExpress is a software-only... gateway (we used a Cisco AS5200 in our tests). The home gateway becomes responsible for **authenticating** the **user** and providing the required network addressing. The remote-access server at the POP simply provides... your virtual backbone. Privacy is typically considered in the context of hiding data from prying **eyes** or tampering. The complete VPN network should be as strong as your internal network. IPSec...

...outsource; for instance, you might want to outsource just the infrastructure while maintaining control over **user** **authentication** and access.
Not only are service providers offering tunneling, but they claim to improve data...more complex for the average user (for example, having to remember more user ID and **password** pairs), the less likely users will be to adopt the VPN strategy.
IPSec technologies require...

...the workstation without knowing who is at the console-there isn't any provision for **user** -based **authentication** . On the other hand, authentication using a non-IPSec solution-such as Aventail Corp.'s...

...user databases such as NT Domains and RADIUS. Users have to be verified using a **password** , token card or other authentication before they can access network services.
Of course, user access is just one piece of the puzzle. Once a **user** is **authenticated** , data traffic needs to be protected as well. Generally speaking, the strength of an encryption...

11/3,K/31 **(Item 15 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)

04954772 Supplier Number: 47281106 (USE FORMAT 7 FOR FULLTEXT)
The National Registry Inc. Introduces Finger-Image Authentication for Laptops
PR Newswire, p0407ATM007
April 7, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 590

... authentication solution for laptop computers.
NRIdentity(TM) Pass for Portables applies state-of-the-art **biometric** identification capabilities, ensuring secure remote access to Intranets and other corporate networks. The integrated hardware...

...Gustafson. "NRI's solutions offer accurate, user- friendly finger-image identification which meet the serious **challenges** of **verifying** authorized users of corporate Intranets and other distributed client/server networks. Finger imaging also provides a convenient and affordable alternative to traditional methods of **user** **authentication** which are easily compromised."
NRI also is approaching the network authentication market through strategic partnerships...

...offers customers of its global corporate Intranet services the added security of NRI finger image **verification** of **user** identity. Key Tronic Corporation, a world leader in keyboard and input device technology, provides the...

...imaging technology to verify individual identity; to protect business and personal information; and to replace **passwords** and PINs to safeguard and simplify access to electronic systems and enable new online services...

11/3,K/32 (Item 16 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04783078 Supplier Number: 47039951 (USE FORMAT 7 FOR FULLTEXT)
Villains in the Vault (PART ONE)
Willis, David
Network Computing, p52
Jan 15, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2340

... some aspect of security; they may check for operating system configuration errors, reveal easily guessed **passwords** , detect intrusion, scan for viruses, authenticate users, examine system logs or block access to Internet...the workflow system, issuing an alert and updating internal SQL databases with the true settings.

Authenticating the **User** Identifying the actual user behind the computer, never an easy task, is getting harder. Station...

...address information is the best most firewalls can offer us.

We also rely heavily on **passwords** as a means of authentication. Yet **passwords** are often easy to guess, sniff off of the wire, grab over someone's shoulder or otherwise obtain. Although operating systems may avoid sending readable **passwords** over the network during login, applications such as telnet typically pass secrets in clear text. Ironically, many network devices still rely on static **passwords** and telnet for remote administration, providing a rich lodestone for hackers to attack.

Some operating systems, such as Windows95, cache **passwords** locally. In theory, this should minimize the number of **passwords** users must remember and enable them to choose less obvious **passwords** . However, many users don't realize that they still need to protect desktop **passwords** , which they perceive as nothing more than a way to identify a desktop configuration (they...

...that it protects file system access, which it doesn't). Since cascaded host and server **passwords** are not assigned the value of the desktop **password** , the "hidden" **passwords** are often forgotten when it's time to change the server **passwords** or use a different workstation.

Handheld **password** generators, also known as hardware tokens, which generate one-time **passwords** , remain one of the most cost-effective methods of securing systems (see "Desperate Times Call...

...is they don't require special desktop hardware, so they're portable. They generate dynamic **passwords** in a variety of ways, such as challenge-and-response systems that require the user...

...results to the server for acceptance, or simply by going down a common list of **passwords** , la Bellcore's S/KEY (documented in IETF RFC 1760). The most popular security token, Security Dynamics' SecurID, uses proprietary time-based technology to one-time **passwords** in an easy-to-use manner.

Unfortunately, hardware tokens are obtrusive to the user and...

...software-based versions of many hardware tokens are available. The user-shielded from the actual **password** dialog-need only enter a **PIN** to

activate these tokens. It's wise to limit them to desktops where software is reasonably secured, and users should guard their **PIN** from over-the-shoulder snoops.

Smart cards, another excellent authentication method, have many other functions...

...it into the modem saves money and slots; but it's susceptible to the same **PIN** -stealing methods as software tokens.

Biometrics , techniques that identify users via their physical characteristics, have long been dismissed as too expensive...

...for some forms-such as fingerprint recognition-have nose-dived. Over the next few years, **biometric** techniques will appear in vertical applications, such as automated teller machines, but they are not...

...consolidate access control for some devices.

The most important standard for perimeter access is Remote **Authentication** Dial-In **User** Service (RADIUS), which first appeared in 1992. Developed by Livingston Enterprises, RADIUS has ...characteristics such as volume of traffic sent and length of time online. RADIUS supports the **Password Authentication** Protocol (PAP), **Challenge** Handshake **Authentication** Protocol (CHAP) and, in version 2.0, SecurID token authentication.

During **authentication** , the NAS passes **user** identification information to the RADIUS server. For valid users with approved access, the server returns...

11/3,K/33 (Item 17 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04545878 Supplier Number: 46680576 (USE FORMAT 7 FOR FULLTEXT)
AssureNet Pathways to Demo Web Page Authentication Technology at Interop; Web Defender Assures That Only Authorized Users Access Restricted Information.
Business Wire, p09031053
Sept 3, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 889

... s Defender Security Systems product line in early calendar Q1, 1997. Unlike static IDs and **passwords** that are used in many Web server products, the Web Defender uses Defender token technology for strong **user authentication** , allowing companies to enhance the security and expand the capabilities of their Web sites by...

...AssureNet Defender Security Server (DSS) upon entry to a secured Web environment. The two-factor **challenge / response** process then performs the **authentication** . Once authenticated, any request for a secure Web page will require that the CGI wrapper...
...will allow companies to require that employees, vendors, customers, and others pass rigorous one-time **password** authentication before viewing protected Web pages. When shipped, the Web Defender will be able to...

...multiple web pages, provide page-level user authorization and provide an audit trail of each **user authentication** . While the first release of the Web Defender will use a hardware key, later versions...

...secure," said Ted Haynes, vice president of product marketing for AssureNet. "By making one-time **password** authentication easy to use on the

Web, AssureNet Pathways is allowing businesses, governments and non...

...similar to the military-type method of information classification, i.e. confidential, secret, top secret, **eyes** only, has wide ranging commercial applications."
Expanding Web Site Capabilities
Companies will use the Web...

11/3,K/34 (Item 18 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04253159 Supplier Number: 46228573 (USE FORMAT 7 FOR FULLTEXT)
Data General-BDM International software alliance produces Internet security breakthrough; DG/UX B2 Security with CYBERSHIELD cost-effectively protects Internet and Intranet business computing.
Business Wire, p3181241
March 18, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1252

... with DG/UX B2 Security and CYBERSHIELD can be configured to enforce a number of **user** identification/ **authentication** procedures, including simple, randomly generated **passwords** , smart cards, hardware and software tokens, public and private key **authentication** systems, digital signatures, **biometrics** and **challenge** /response systems. All these methods are transparent to the client/server software being used.
To...

11/3,K/35 (Item 19 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

01747641 Supplier Number: 42189170 (USE FORMAT 7 FOR FULLTEXT)
ADDRESSING SECURITY
Network Computing, p57
July, 1991
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1555

... getting users to lock their offices and desks at night. Other measures are to change **passwords** periodically, avoid easy-to-guess **passwords** , and prohibit two people from having the same **password** .
Another basic security technique is locking up LAN servers and removing their keyboards and monitors. Another is to use a product's security features: Switch all **passwords** from the ones given at the factory and immediately change other features from insecure default...that much remains to be done and that the work is progressing too slowly.
Fixed **passwords** , which are subject to tapping and other compromises, can be also secured by encryption. Methods...

...the private-key communication to that between a user and a trusted specialized service, which **authenticates** the **user** to the other machines on the network. Besides its role in the Open Software Foundation...

...Kerberos is included in a new version of Sun Microsystem's Open Network Computing environment.
Challenge - response techniques are effective for **authentication** ,

in part because they do not send **passwords** from the **user** to the **authenticating** computer.

Instead, the **user** sends his or her user name. The computer has a key for the user, which...

...retinas, voiceprints or other biological characteristics assumed to be unique to the user. Tokens and **biometric** devices may also require a **password** . Overall, the universal need for some convenient one-stop authentication to replace memorizing many **passwords** and to facilitate flexible distributed processing should build a large market for smart cards or...

...Set and carry out carefully detailed corporate policies on security. Observe all security fundamentals: Use **password** protection, including all the rules necessary for generating good **passwords** ; Ensure proper logoff procedures by authorized users; Ban automatic logons; Protect crucial servers and the...

11/3,K/36 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

11579184 SUPPLIER NUMBER: 19528049 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Who knows who you are? (Network authentication solutions: National Registry's Secure Authentication Facility for Windows NT; Security Dynamics' solution comprised of Ace Client for NT, Ace/Server 2.3 and SecureID Token; and Vasco Access Control Manager) (includes related articles on summary of results, basic ownership costs and notes from the test center) (Software Review) (Evaluation)
InfoWorld, v18, n24, p108(10)
June 16, 1997
DOCUMENT TYPE: Evaluation ISSN: 0199-6649 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 8817 LINE COUNT: 00917

... to leak out or lose? If so, you may need something more than your simple **password** system to keep it safe from internal attack.

Computer security is a never-ending pursuit...

...break-in. Twenty-one percent said their companies' internal networks have experienced an internal breach.

PASSWORD LIMITATIONS. So what are IS managers doing to deal with this increasing threat of internal security breaches? Today, almost 80 percent of corporations use **passwords** as their main method of security. **Passwords** are popular mainly because they're included free in every major network operating system (NOS).

In theory, if **passwords** were used effectively, they would provide a very high degree of security, but in practice they're not used properly at all. And there, precisely, is the problem. **Passwords** have limitations; they're easy to guess, people are reluctant to change them, people write...

...the same one for multiple functions, and often they are not administered efficiently. In short, **passwords** are vulnerable to attack.

There are several new authentication methods on the market that promise to either supplement **password** security or replace it. In this Comparison we focus on solutions from the two most-important categories: authentication tokens and **biometrics** . Authentication tokens beef up security by requiring the user to present a physical object in addition to supplying a user name and **password** to gain network access. **Biometrics** involves authenticating users to a network based on a physical characteristic unique to each individual, such as fingerprints,

handwriting, voice, and facial feature's. In essence, with **biometrics** the users are the **password** .

When we set out, we decided to focus on solutions that provide NOS-level integration...administrators the option to continue allowing users to log in with a user name and **password** when first switching over to fingerprint identification. This allows for a gradual and less painful ...

...you can disable finger authentication and let them log in with a user name and **password** . This feature is available even on the same machines that other users are logging in...need to add another server to handle file and print services.

SecurID Tokens use a **response** -only method to **authenticate** users to the computer network. **Response** -only tokens use time to generate a code. The token is registered with the server...

...a screen appeared the first time we logged in that allowed us to create a **personal identification number** (**PIN**) for the token we were using. Administrators can configure the system to allow users to select their own PINs, or they can instruct the server to generate the **PIN** . They can also specify the length of the **PIN** and whether or not it contains letters or numbers or both. When users are presented with the token screen at the next log-in, they enter their **PIN** and the code that appears on the token.

Smart features and unsuspecting hackers

We liked...

...SecurID, unsuspecting hackers might be able to log in and discover a user name and **password** for the workstation they're on, but after the GINA screen disappears, they will be...

...not offered by the other two solutions in our Comparison. If you enter an incorrect **PIN** but a correct token code when you are presented with the token screen, the server...

...code was entered. If the token code is correctly entered three times with an incorrect **PIN** , the server assumes that the token has been stolen and denies access. If the token...

...in the works but did not say when it would be implemented.

Step by step

Response -only (time-based) token **authentication**

How the Security Dynamics solution works

1 User presses Crtl-Alt-Del to long on...

...with domain name.

3 User enters user name (if different from previous log-on) and **password** for Windows NT.

4 PDC accepts user name and **password** .

5 Ace/Server prompts for **personal identification number** (**PIN**) and token code.

6 User enters **PIN** and code currently displayed on SecurID Token.

7 Ace/Server generates token code for the time the **user** logged in and **verifies** this code against the code entered by the user.

8 User is logged on to...

...server (VACMan Server 2.0 and the AccessKey II Token). This solution uses the Remote **Authentication** Dial-In **User** Service (RADIUS) protocol to handle transactions between the client and server. Unfortunately, Vasco failed to...for this Comparison. The Vasco solution differs from the Security Dynamics solution in that it **authenticates** using the more complex **challenge - response** token. As with the Security Dynamics solution, the token is registered on the server, and the algorithm for generating token codes is also registered on the server, but the **challenge**

- **response** method of **authentication** does not depend on time.
VACMan Server runs on Windows NT 3.51 and NT...

...of authentication is a three-step process. The user enters his or her user name, **password** , and domain name into the log-in window and selects OK. If the server accepts the user name and **password** , a one-time **personal identification number** (**PIN**) is passed back to the client and appears on the log-in screen. To enter...

...number and calculates the response from it.
We liked this painfree method of entering the **PIN** into the token. If the server receives the response that it expects from the token...

...Although VACMan Server let us deny access after a certain number of bad logins -- either **passwords** or token codes -- its lockout mechanisms aren't as sophisticated as those of the Security Dynamics solution. For example, it doesn't detect when a hacker is entering correct **passwords** but incorrect token responses, unlike the penetration-evasion features of the Security Dynamics solution.
Real...

...reasonably strong solution for IS managers looking to improve their network security.
Step by step
Challenge - response token **authentication**
How the Vasco solution works
1 User presses Ctrl-Alt-Del to log on.
2 User enters user name, **password** , and domain name.
3 Primary Domain Controller (PDC) checks user name and **password** .
4 If user exists and **password** is correct, VACMan Server generates and sends one-time **password** to the client screen.
5 User enters this one-time **password** into token (or reads it in a bar code off the screen). The token calculates...

...that the user types on the keyboard and clicks OK.
6 VACMan Server generates token **response** and **verifies** this code against the code entered by the user.
7 User is logged on to...

...in the domain was easy. Letting users log in with only a user name and **password** until the system is up ...easy. In fact, we found that using SAF NT was easier than authenticating with a **password** Users on their own workstation don't even have to type their user names in...

...of administration features with NT. We liked the capability to enable tokens with a"new **pin** mode," allowing users to choose their own secret codes. All events are logged, and the...

...Very Good (=) 1.2 operation Using the SecureID card was simple; we typed in our **personal identification number** (**PIN**) and token code. Like the others, this solution integrates with the screen saver, so

we had to re-authenticate each
time we unlocked our workstation.
Changing a **PIN** requires an administrator,
because you can't link the new **PIN** mode
to the Change **Password** routine.

Reliability ?? Satisfactory (=) 1.4
A security loophole adversely affected
this score. We could not...

...another platform to
VACMan, but we would prefer a single log-on
system whereby a **user** is **authenticated**
first to and then ...user Good (=) 0.9
operation We liked the way AccessKey II Token
reads the onetime **pass code** off the screen and
automatically generates a **PIN** from it. But
VACMan doesn't remember the last user or the
last domain logged...

...had to type
in our user and domain names each
time. If you have a **password** in addition
to Access-Key, there's no way to change
it from the client...found that although the product
works well in controlled situations, many factors can affect a **user** 's
ability to **authenticate** .
Voice Guardian's window for registering users is similar to the
windows used to calibrate...

...is not set correctly, the program won't understand you. You have to say
your **password** in the same tone and with the same modulation as when you
registered with the...
...In order to make your network more secure, you can require users to
change their **passwords** frequently.
VACMAN
If the administrator enables VACMan's proxy option, the system, after
checking the...

...Comparison we had the opportunity to look at two of these technologies:
authentication tokens and **biometrics** (in this case, fingerprint
authentication).
Tokens augment network security by requiring users to possess
something in addition to knowledge of a **password** , for example. To
authenticate to the network, users must present a token at log-in...

...for the server varies from one token to the next. We looked at two
diverse **authentication** token solutions: **response** -only tokens and
challenge-response tokens.
The key piece of each of these implementations is...

...codes. This is where security is enforced and maintained. Each method
generates one-time, unpredictable **passwords** based on the carefully
guarded algorithm. With response-only tokens (time-based), the token has...
...on the correct response from the token to a "challenge" from the server.
By contrast, **biometrics** rely on a person's distinct physical
attributes, such as a fingerprint, to positively identify...

...by a token can be 100 percent verified on the server, the "code"
generated by **biometric** solutions will only approximate the value stored
on the server, and an algorithm must decide...

...the values are close enough. However, along with absolute verification of tokens comes a disadvantage. **Biometric** solutions rely on an essential part of you that can't be stolen or lost...

...its fingerprint-authentication technology was impressive enough to suggest that this solution in particular and **biometrics** technologies in general may have a bright future in the area of personal authentication.
National...

...solution proved to be relatively painless. We actually found it easier to use than a **password** system: There are no phrases or secret words to remember; just set down your finger...In this way, a hs 95 machine with knowledge of the authorized user name and **password** could gain access to the server being protected by the Security Dynamics solution and the...
...security weaknesses of network operating systems (in this case, Windows NT) and the frailty of **password** systems in general. **Passwords** can be guessed or stolen, and most network OSes (NOSes) have built-in security flaws...

...on the system, but it might interrupt work if scheduled too close to business hours.
PASSWORD STRATEGIES. Locking down users' accounts if they enter **passwords** incorrectly a certain number of times within a specified amount of time is a way...

...amount of time can help relieve the administrative burdens caused by users who type their **passwords** incorrectly. Requiring users to change their **passwords** periodically will certainly make your network more secure. But if you allow them to recycle **passwords** that they have used before, requiring **password** changes has no benefit.
Making users learn a new **password** every month could cause some to resort to writing them down, compromising the very security...

...no substitute for augmenting your security with a product that eliminates the problems associated with **passwords** .

11/3,K/37 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

11336348 SUPPLIER NUMBER: 55730429 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Enterprise Communications Start Migration To VPNs. (IT survey) (Industry Trend or Event)
InternetWeek, NA
Sept 13, 1999
ISSN: 1096-9969 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 8283 LINE COUNT: 00637

... to support the same Certificate Authority. Similarly, if remote users already use tokens or dynamic **passwords** , the VPN gear will need to support the same systems.
Fortunately, most of the VPN...

...resilient security technologies.
Ninety-three percent of IT managers said they use user names and **passwords** for access ...is one of the cornerstones of every VPN.
Many IT managers are keeping a close **eye** on what they foresee as a problem in the future when they start using more...that for a premium service.

VPN Acronyms

ATM -Asynchronous Transfer Mode
CA -Certificate Authority
CHAP - **Challenge** Handshake **Authentication** Protocol
DES -Data Encryption Standard
DHCP -Dynamic Host Configuration Protocol
DNS -Domain Name Service
EDI...

...Point-to-Point Compression
MPPE -Microsoft Point-to-Point Encryption
NAT -Network Address Translation
PAP - **Password** Authentication Protocol
PKI -Public-Key Infrastructure
POP -Point Of Presence
PPP -Point-to-Point Protocol...

...to-Point Tunneling Protocol
PSTN -Public Switched Telephone Network
QoS -Quality of Service
RADIUS -Remote **Authentication** Dial-In **User** Service
SKIP -Simple Key Management For IP
SLA -Service Level Agreement
SSL -Secure Sockets Layer...

11/3,K/38 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10282482 SUPPLIER NUMBER: 20841470 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Security -- Sign On Here -- Single sign-on systems can help seal IT security while boosting worker productivity and improving enterprise management. (Technology Information)
Davis, Beth
InformationWeek, n688, p54(1)
June 22, 1998
ISSN: 8750-6874 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2183 LINE COUNT: 00177

TEXT:
...workers access everything from E-mail to high-end production applications using one ID and **password** .
... logons.
As client-server applications have proliferated, so have the number of user IDs and **passwords** needed to access them. Character lengths vary, and different systems and applications carry different **password** -expiration processes. One result is that users often write down their many IDs and **passwords** and stick them on their computer monitors-despite business IT security policies that forbid this...
...the sector to achieve rapid growth, despite widespread recognition of the 'too many IDs and **passwords** ' problem," Gartner analyst Helen Flynn says in her report.
Vendors seeking to convince jaded IT...object interceptor, in which the targeted system presents its request for a user ID and **password** via a set of user interface components. The single sign-on system stores that data in an object identifier, plus the associated user ID and **password** . When the object identifier is invoked by a user attempting to log on, the **user** is **authenticated** and then the relevant **password** is plugged in to open a session. With these types of systems, IT departments don...

...link single sign-on systems with back-end systems and applications.
The addition of standard **authentication** methods such as the

Challenge Handshake **Authentication** Protocol and others means better interoperability among the various systems. Also, most current single sign ...

...summer. The next release will support alternative authentication methods such as fingerprint readers and other **biometric** mechanisms as well as smart cards. IBM also plans to support SAP and other enterprise...

...to move beyond single sign-on to become a provider of systems that also cover **password** synchronization, security, and information access.
Others are also marketing their single sign-on software as...

...controls on a number of systems and applications, as well as synchronize user IDs and **passwords** . Control-SA doesn't reduce the number of **passwords** , but it does help an IT organization centrally manage everyone's **passwords** and access mechanisms.
Information Repository
Here's how it works: Agents are installed on the...

...to manage. These agents gather information from the system and populate a repository with the **passwords** and user IDs that are authorized to the system. For example, an NT system knows which user IDs and **passwords** are allowed to access it, and it keeps that information in a secure user database...

...from any location. Control-SA also lets IT shops sync up the various end-user **passwords** .
Unlike native access, in which a user logs on directly to the application or system, **password** synchronization requires the end user to log on to a subsystem, such as Control-SA, which then matches that user's logon and **password** information, which is held in the repository, with all the various back-end systems the user has authority to access. "With **password** synchronization, when a **password** is changed, Control-SA will change all the other **passwords** ," Shannon says.
Companies with successful single sign-on implementations say the payback is substantial in...

...by Forrester Research Inc. suggests that as much as 80% of help-desk calls are **password** -related. Single sign-on systems could enable a company to reduce its help desk by...

11/3,K/39 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

09931564 SUPPLIER NUMBER: 20061975 (USE FORMAT 7 OR 9 FOR FULL TEXT)
VPN growing pains. (six remote access solutions reviewed) (includes related article on test results) (Hardware Review) (Software Review) (Evaluation)
InfoWorld, v19, n49, p102(12)
Dec 8, 1997
DOCUMENT TYPE: Evaluation ISSN: 0199-6649 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 9461 LINE COUNT: 00782

... Security 20% -- Very Good = 1.6
AccessBuilder's out-of-the-box authentication is strong. **Passwords** and callback phone numbers can be set for remote users. AccessBuilder also supports several third-party security services, but not Remote **Authentication** Dial-In **User** Services (RADIUS). Its security auditing tools could be more elaborate.
Performance 20% -- Very Good = 1...Tunnel 97's authentication,

achieved via RSA public-key exchange, is bidirectional. Public keys are **password** protected, establishing an effective "two factor" identification requirement for tunnel connection. Tunnel 97 implements a...only weak point in terms of security is AccessBuilder's lack of support for Remote **Authentication** Dial-In **User** Services, or RADIUS.

As one would expect from a solution unencumbered by encryption and the ...rekeyed. Eagle NT provides for many authentication options, and it even allows sequences of different **authentication challenges** to be set up, but the two methods we tried were unsatisfactory. We initially used NT domain authentication, but we later learned that **passwords** are sent in clear text via the Internet. We then tried Eagle NT's built-in support for S/Key **challenge / response authentication** , but we could never reliably verify that it was working correctly, even with Raptor's...the best VPN solution in our comparison. In conclusion, we have to say keep your **eyes** on hardware VPN providers such as VPNet, but for now keep your hands on your...

...convenience (we're pretty sure all administrators would love to answer those requests to change **passwords** while browsing the Web from a vacation hideaway).

On the security front, ANS' claims to...tacked on its own solution for securing PPTP sessions. We liked the availability of Microsoft **Challenge** Handshake **Authentication** Protocol, or MS-CHAP, for our Windows clients, because it uses hashed **user** credentials for **authentication** and derives encryption keys from the same hash locally. This keeps sensitive user information and...

...category: difficulty in determining the encryption key length being used; lack of built-in Remote **Authentication** Dial-In **User** Services, or RADIUS, support; lack of a decent security monitoring utility; and the lack of...in that it encrypts IP packets as they exit the network layer.

Authentication is via **password** -protected RSA public key exchange, session encryption uses RSA's Rivest Cipher 4 (RC4) algorithm...be matched by its less-mature VPN competitors. Other than lack of support for Remote **Authentication** Dial-In **User** Service (RADIUS), it is hard to find anything negative to say about the AccessBuilder 4000...

11/3,K/40 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08759997 SUPPLIER NUMBER: 18310211 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Spies like us. (increasing internet security risks, corporate sabotage) (includes related articles on increasing security, a glossary and information resources) (Internet/Web/Online Service Information)
Young, Jeffrey
Forbes, v157, n11, p70(14)
June 3, 1996
ISSN: 0015-6914 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 8225 LINE COUNT: 00664

... peeking at proprietary information can be awfully tempting. Randal Schwartz, and contractor, was caught cracking **passwords** on a system he wasn't authorized to access. Intel discovered this activity and reported...

...altering Intel's computer system and two of knowingly using a computer system to steal **passwords** . On September 11, 1995, Schwartz was sentenced to five year-e' probation with special conditions...at the push of a button. But they can also be programmed to send out **passwords** or credit card information you used while cruising the Web, or to list all the...

...searching for strings like "root:" end up getting copies of entries from

the server's **password** file. The attacker then runs a **password** -guessing tool, such as Crack, and gains unlimited access to the server and its data ...

...activities that allows activities to be reconstructed.
Authentication: Determining the identity of a communicating party.
Biometric Device: Autheticates a user by measuring some hard-to-forge physical characteristic, such as a...

...into a telephone system to make calls that bypass billing procedures.
Brute Force Attack: Hurling **passwords** at a system until it cracks.
Challenge -Response: A type of **authentication** in which a **user** must respond correctly to a challenge, usually a secret key code, to gain access.
Computer...

...collect a certain number of bytes from the beginning of each session, usually where the **password** is typed unencrypted.
Social Engineering: Gaining privileged information about a computer system (such as a...

...a company).
War Dialer: A program that tries a set of sequentially changing numbers or **passwords**) to determine which ones respond positively.
RELATED ARTICLE: MOST WANTER
Ninety-one percent of all...

...in Carlisle, Penn. He specializes in social engineering, the art of talking employees out of **passwords** and information. Major corporations hire him to attack their computer security infrastructure. With the information...

...knows the location of the most sensitive files on the network. The minutes include the **password** and log-on ID for a master document required by a government agency. The document...network. The portable is loaded with programs, including one that identifies accounts with easily guessed **passwords** . Using one of these accounts, Winkler logs onto a server, and with another hacker tool...

...log off her computer and then log on again, he is able to guess her **password** . Back in his office, he logs on using her ID and accesses central files detailing...simple burglary.
Have someone monitor references to your company on the Web. Also keep an **eye** on Usenet newsgroups for slander, libel and unwitting disclosure of proprietary information by employees.
Agree...happened at a database company.) Or how about the guy who keeps getting the evil **eye** from clients whenever he shows up for appointments? One day he notices that changes have...

11/3,K/41 (Item 6 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08557577 SUPPLIER NUMBER: 18131001 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Internet security: Data General-BDM International software alliance produces INternet security breakthrough; DG/UX B2 Security with Cybershield protects Internet and intranet business computing. (Product Announcement)
EDGE: Work-Group Computing Report, v7, n13, p20(1)
March 25, 1996
DOCUMENT TYPE: Product Announcement LANGUAGE: English

RECORD TYPE: Fulltext
WORD COUNT: 1224 LINE COUNT: 00108

... with DG/UX B2 Security and CYBERSHIELD can be configured to enforce a number of **user** identification/ **authentication** procedures, including simple, randomly generated **passwords** , smart cards, hardware and software tokens, public and private key **authentication** systems, digital signatures, **biometrics** and **challenge** /response systems. All these methods are transparent to the client/server software being used.
To...

11/3,K/42 (Item 7 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

03933571 SUPPLIER NUMBER: 07494095 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Who goes there? (user - verification systems to restrict access to computer data) (special section - Computer-Information Security: Getting the Protection You Need)
Mayfield, Charles
Security Management, v33, n2, p36A(3)
March, 1989
ISSN: 0145-9406 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2007 LINE COUNT: 00164

Who goes there? (user - verification systems to restrict access to computer data) (special section - Computer-Information Security: Getting the Protection...
... users and, in many cases, against viruses. One computer security approach is to require a **user** to be **verified** before gaining access to a computer system or application. This is commonly known as a **user - authentication** system.
BASICALLY, THERE ARE THREE types of **user - authentication** security systems for computers in network environments: logic-based systems, hand-held key token devices, and **biometric** systems. Each system functions by confirming that the user who wants to gain access to...

...fact, authorized to gain access.
Logic-based systems. These are typically software-based systems using **passwords** that rely on what a **user** knows to determine **authentication** . While easy to implement, **password** systems are very difficult to secure. For one thing, **passwords** can be fairly simple to decipher. People often use names, anniversary dates, and other **passwords** that are easy for the user to remember--and also easy for someone else to figure out.
In addition, users write **passwords** down so they don't forget them. Once written, the **password** may be seen by anyone and, once public, all protection is lost. Repeated use of the same **password** and the sharing of **passwords** among users also threaten their effectiveness.
For management and administration, **password** security systems can be more trouble than they are worth. Management must assign and eliminate **passwords** to keep pace with employee turnover. They may also want to issue multiple IDs to grant individual users special privileges, depending on their job functions.
An extended **password** algorithm system offers an alternative to memorized **passwords** , but it also is difficult to administer. In an algorithm-based security system, the user...

...is "dog."
In the algorithm system, each challenge is unique, so the problem of exposing **passwords** is limited. However, administration of the algorithm system is cumbersome and raises some difficult questions...

...are programmable, hand-held devices, which are used in conjunction with a user ID and **password** . A separate key is assigned to each user. Then, when software on the host computer issues a challenge, the key is used to provide a proper **response** .

In one particular key token **authentication** device system, the host issues a challenge via a flashing light pattern that represents a...

...the flashing pattern, read and process the random number. The access key then displays a **password** on its LCD screen. The user enters this **password** on the computer terminal keyboard. If the correct key has been used for the corresponding...

...granted.

One of the benefits of this system is that the software generates a unique **password** with each use, making it impossible for a user to guess a **password** . The key will operate on mainframes, minicomputers, and PCs.

In addition, management can allow a...

...specific data bases, applications, and networks.

The token key approach provides greater security than the **password** approach and is suitable in settings that require moderate levels of security and in mobile...

...used to protect a company's proprietary product information, financial data, and consumer market information.

Biometric authentication systems. These systems provide the highest level of security. They incorporate hardware and software...

...corporate accounting records. Corporations with large, centralized data bases are becoming more common users of **biometric** security systems.

Active **biometric** systems analyze the user's personal characteristics to determine whether access is permissible. Characteristics such...

...unique to the individual; they cannot be stolen, forgotten, written down, misplaced, or duplicated. Hence, **biometric** systems that use these characteristics provide an extremely high level of security. Passive **biometric** systems analyze characteristics related to behaviors to **authenticate user** identification. For example, a typing sensor system measures a person's typing pressure and speed...

...the data, and compares it to the stored fingerprint data.

From an administrative perspective, a **biometric** system requires minimal management. Unlike the **password** system where the user must routinely protect and change his or her **password** , a **biometric** characteristic will not change, so user IDs do not have to be changed periodically. (However...

...mistakenly grants access to an unauthorized user, and false denials were a problem for early **biometric** systems. Today's technology has improved on the accuracy of early versions. However, the technology...

...be successful, the company's needs and the effectiveness of each technology should be considered. **Passwords** , token devices, and **biometrics** provide different levels of security. It is not necessary to purchase a high-level security...

...key factors, if considered early in the planning process, will help make implementation of a **user - authentication** system successful. These factors should be considered for any extended **user authentication** system, whether token-based or **biometric** .

First, define precisely what should be protected and to what degree. Should all organizational data...

...A mix of authentication systems may be most appropriate. A combination of token systems and **biometrics** provides a higher level of security. Or, different technologies may be applied to computers that...

...with access to organizational data make in-house data bases and networks vulnerable to tampering.

Password protection may be the solution, or it may be too vulnerable and labor-intensive for...

...provide a higher level of security and are particularly well suited for dial-up networks. **Biometrics** provide the highest level of **user verification** and can not only augment but in some cases actually replace **password** protection.

Whichever solution the company chooses, the most important point is to secure access to...

11/3,K/43 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02418496 SUPPLIER NUMBER: 62266765 (USE FORMAT 7 OR 9 FOR FULL TEXT)
2000 Products of the Year Award Winners.
Network Magazine, NA
May 1, 2000
ISSN: 1093-8001 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 12704 LINE COUNT: 01053

... order to talk, customers and vendors have to negotiate a bevy of firewalls, VPN clients, **password** dialogs, certificate infrastructures, and more.

The vision driving adoption of directories is that, once they...

...was hence acquired by Legato Systems.)

The product still has the features that caught our **eye** last year- bidirectional failover, the option of both active/active and active/passive configurations, well...PKI compatible.

The system includes support for many companies' digital certificates. It also supports Remote **Authentication** Dial-In **User** Service (RADIUS), **Challenge** Handshake **Authentication** Protocol (CHAP), and **Password** Authentication Protocol (PAP), as well as RSA's SecurID tokens.

www.vpnet.com
Authentication
ClearTrust...

...SecureControl includes a single sign-on capability and supports multiple authentication methods, such as username/ **password** , digital certificates, and tokens. Permissions can be established at the server, directory, application, or Web...for signs of an intrusion. Host-based systems monitor specific local machines and keep an **eye** out for activity that deviates from predefined parameters.

RealSecure 3.2 from Internet Security Systems...including digital signatures, RSA encryption, server authentication prior to transmission, a document expiration date, and **password** protection. In addition, the Tumbleweed IME developer toolkit lets in- house developers customize IME-enabled...

...and encapsulated into Real-Time Transport Protocol (RTP) packets. A service provider can use Remote **Authentication** Dial-In **User** Service

(RADIUS) servers for authentication, authorization, and billing.
The AS5300 also has the smarts to

11/3,K/44 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02411229 SUPPLIER NUMBER: 62790289 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Healthcare Security Regulations.
Rabinovitch, Eddie; Pawola, Larry
Enterprise Systems Journal, 15, 6, 52
June, 2000
ISSN: 1053-6566 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2971 LINE COUNT: 00261

... is not just an IT issue; it's an organization-wide initiative.
CSF 2 -- Secure **User Authentication** . Using identifiers, **passwords** and other devices (e.g., **biometric** systems) to control who can access patient data in your computer system.
CSF 3 -- Access...the benefits of networked data communications must contain these elements:
* Physical protection -- Where are you?
* **User authentication** -- Who are you?
* Access control -- What asset(s) are you allowed to use?
* Encryption -- What...

...determine who is authorized for what kind of access to which information
* Employ a strong **user - authentication** system
* Deny malicious or destructive access to any information asset
* Protect data from end to...

...of any security system. It's the only way to differentiate authorized users from intruders. **User authentication** to the network is a necessity for any enterprise that is serious about protecting information...

...following elements:
* What the user has or possesses (smart card, certificate)
* What the user knows (**password**)
* A physical attribute (fingerprint or other **biometric** information)
Authentication is most often achieved through **challenge** and response, digital certificates, or message digests and digital signatures.
Protection from the Outside
Access...inform users of their responsibilities; corporate policies defining network access, service access, local and remote **user authentication** , dial-in and dial-out, disk and data encryption, and virus protection measures; and employee...

11/3,K/45 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02155115 SUPPLIER NUMBER: 20417017 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Now, That's a Secure VPN. (Aventail's Aventail VPN 2.5 virtual private network software) (Software Review) (Evaluation)
Phifer, Lisa A.
Windows Sources, v6, n4, p118(1)
April, 1998
DOCUMENT TYPE: Evaluation ISSN: 1065-9641 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1345 LINE COUNT: 00112

... other Socks 4 or 5 server). In turn, the VPN server intercepts TCP and UDP (**User** Datagram Protocol) traffic, **authenticates** the **user** , and determines whether to grant access to the specified destination based on access controls and...

...For server authentication, we used SSL, and for client subauthentication, we chose CHAP (the popular **Challenge** Handshake **Authentication** Protocol many ISPs use) from the long list of supported methods, which include NT domains, RADIUS (Remote **Authentication** Dial-In **User** Services), and SecurID/ACE.

Then we implemented a security policy that permitted HTTP access to... CHAP challenge (a request that requires the client to respond with an authorized username and **password**). Once the client responded correctly to this challenge, the VPN server established a proxied connection...

...Traffic Monitor (see the screenshot on the first page of this review) to keep an **eye** on VPN activity. The VPN Traffic Monitor displays active and failed connections and real-time...

11/3,K/46 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02075155 SUPPLIER NUMBER: 19500445 (USE FORMAT 7 OR 9 FOR FULL TEXT)
A new way to authenticate users. (Visage Developments' Visage 4.0 authentication software) (Software Review) (Evaluation)
Cobb, Michael
Databased Web Advisor, v15, n6, p70(2)
June, 1997
DOCUMENT TYPE: Evaluation ISSN: 1090-6436 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1219 LINE COUNT: 00095

...ABSTRACT: 4.0 authentication software is an easy-to-install and administer solution that provides genuine **user** **authentication** . The software relies on users be authenticated by identifying three key faces from a total...

...is a fun solution that is certain to help administrators frustrated with lost or forgotten **password** requests. The application requires no additional hardware, but the enrollment script is a bit basic...
... to be. Thus, the problem of access control is really one of authenticating users.

Traditional **passwords** and PINs can be exposed by users who write them down, divulge them to others and, in the case of tokens, have them stolen. Yet, **passwords** and PINs don't necessarily ensure that people really are who they say they are...

...they select from a library of images. When a user logs on and enters his **user** ID, Visage **authenticates** the **user** by getting proof of identity. Assuming a basic setting of one key face in a...

...way, and then the third. If all the key faces have been correctly selected, the **user** is **authenticated** . Each time the **challenge** is run, the key faces appear in different positions, so the actual keys pressed are ...

...groups. Once the users are added, administrators can set their security configuration.

The user's **password** configuration and resulting level of security

is set on the New Grid page (figure 2...

...setting, so it isn't too much of a rush for users to move their **eyes** from screen to keypad (using the mouse was the easiest for me).
Levels of security...

...and from there you must log on to the system using your Visage 4.0 **password** . This enrollment process is easily customized by changing the enrollment script.
How does it handle...faces. After that, I increased the security levels and had no problem remembering the different " **passwords** ." It's fun to use, and I tested several friends--before and after a few...

...the system to use Visage 4.0, as it also allows users with just text **passwords** to log on, too. Visage plugs into your screen saver, and by pressing Control+Alt...

...use, and definitely helps increase security, particularly among non-security conscious computer users. What better **password** than, "I can't describe it, but I'll know it when I see it...

...system administrator, it's easy to setup, and greatly reduces the time wasted on forgotten **passwords** , or lost tokens, while providing true **user authentication** .
Let's face it. This is security with a difference.
Michael Cobb owns CobWeb Applications...

11/3,K/47 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01890677 SUPPLIER NUMBER: 17488771 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Internetwork 1995 TCP/IP software directory. (Internetwork supplement) (includes company index) (Buyers Guide)
INTERNETWORK, v6, n8, pA1(20)
August, 1995
DOCUMENT TYPE: Buyers Guide LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 14920 LINE COUNT: 01298

... can log on, and whether or not users can read or write to specific files. **Password** encryption, forced logout, simultaneous login restrictions, audit trails and other features ensure full protection against...problem solving.
* Vital Signs LOCKout
Vital Signs Lockout is a software product that uses a **challenge** / **response** mechanism to **verify** the authenticity of users signing on to computers and networks. It runs on popular client...

...TCP/IP networking applications to work without modification. Remote access is authenticated by one-time **passwords** using tokens.
Cabletron Systems 35 Industrial Way Rochester N.H. 03866 (603) 332-9400
* Spectrum...and server solutions for authenticating in ways that are more secure than traditional Ids and **passwords** . All Defender systems are managed by a Windows-compatible management application. The Windows Defender Management using their own address books.
Diversified Computer Systems
3775 **iris** Ave., Suite I B
Boulder, Colo. 80301
(303) 447-9251

* EM320 for Windows * EM340 for...NetSP) V1 R2 provides security across a distributed network. It eliminates security exposures with no **passwords** ever flowing in the clear and provides one standard graphical interface to secure IBM, HP...

...services with the Socks server; provides gateway authentication with proxy servers; provides a choice of **authentication** method for each **user** ; offers advanced filtering capabilities; and has menu-driven panels to provide flexibility in controlling traffic...are updated or reconfigured by a software utility and can be protected with an optional **password** . One package of BootWarePLUS supports many different LAN adapters, including NetWare, Unix, LAN Manager, LAN...full logging and report generation, and can restrict access based on IP address, username and **password** .

Quadritek Systems 3 Andrew Lane Lansdale, Pa. 19446 (215) 822-8463

* QIP IP Infrastructure Management...systems. Secure/IP protects TCP/IP networked systems by authenticating remote users without exposing their **passwords** in clear text on the network. With Secure/IP, the traditional OpenVMS **password** is replaced with a hand-held or software "token" and a one-time **password** providing two-factor authentication. It provides seamless integration by extending the normal OpenVMS login facilities...

11/3,K/48 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01261220 SUPPLIER NUMBER: 07003427 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Five ways to secure your network.
Weiss, Jeffrey
Telecommunication Products & Technology, v6, n9, p68(3)
Sept, 1988
ISSN: 0746-6072 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1797 LINE COUNT: 00153

...ABSTRACT: technology is easily incorporated into a data communication system and runs transparent to the user. **Biometric** devices have not yet received widespread acceptance because of user frustration and they are frequently unreliable. Many **biometric** systems also use encryption for extended security. **Password** and **biometric** protection can frequently be circumvented.

... securing the network against intruders. At present, there are five common methods:

* Encryption/message authentication
* **Biometrics** (with or without encryption)
* Authentication tokens
* Auto callback
* **Password** entry

If there is concern with unauthorized information disclosure or alteration of data in transit...

...heavy use of encryption for the protection of both fund-transfer messages and user-entered **personal identification numbers** at automated teller machines. Most other commercial users have resisted encryption for reasons focused around...

...encrypted error-free communications path is automatically and transparently established at first connect, and the **user** is **authenticated** . In addition, the system includes extensive centralized network management and access control capabilities.

Other encryption...

...such companies as Racal Milgo, Paradyne Corp., Atalla Corp., ASC Communications Systems and Jones Futurex.

" **Biometrics** "--biological measurements--have been called the technology of the future for the absolute authentication of...

...addition, the units usually have not been attractively priced.

Unless encryption is also employed, passing **biometric** information to a host for validation is nearly as insecure as conventional **password** entry systems, since the **biometric** data may be recorded from the line and replayed at a later date to gain unauthorized access.

Biometric technologies do hold substantial promise for the future. For this promise to be realized, however, system reliability must be increased, costs reduced and encryption incorporated.

Authentication tokens validate a **user** by generating a one-time **password** for each log-on session. This technique prevents intruders from replaying a known **password** to access the network. Devices that implement this technology are typically smaller than a pocket...

...Dynamics Inc., uses an internal clock and a previously entered "seed" to generate a pseudorandom **password** that automatically changes every minute. The user's handled card continuously displays the changing **password** , which, along with a fixed **password** , is manually entered into the computer's or network's terminal/PC keyboard for validation...

...the user is presented with a random number. The user inputs this number and his **password** into the keypad of a handheld, calculator-type device and reads the device's response...

...tokens that can read the challenge value from a CRT and display the proper validation **response** .

Most **authentication** token systems are based upon cryptography. They are therefore difficult, though not impossible, to defeat...

...encrypted or authenticated, it can be intercepted and attacked, bypassing security.

Authentication tokens and encrypted **biometrics** provide a reasonably high confidence level that the user authorized to gain access to a...

...will be picked up by a secretary rather than automatically by the user's modem.

Password entry systems, once the mainstay of computer security, have become the successful target of most...

...systems are too easily defeated. There have been numerous articles written on choosing the right **password** and protecting it from unintended disclosure.

Experience shows, however, that needing the right **password** to access a network is much like needing the right set of keys to drive a car. There are ways to circumvent these requirements, so **passwords** and keys are, t best, deterrents to information and auto "theft."

Assuming you purchase an...

...In general, users are identified to a system when they enter a user ID and **password** . The computer's operating system and security package are responsible for restricting each user's specific access within the system. If one individual uses another's valid ID and **password** , then access will be gained to that particular user's allowed resources.

Token-based or **user** -specific encryption/message **authentication** systems may be " **challenged** " by the computer's own security package to validate a **user** ID. This **verifies** that the **user** has the right to access the requested resource. This ability also allowed mixed-mode operations...

...hackers are your only concern, then token-based or automatic call-back systems are appropriate. **Password** entry systems alone are difficult to justify in today's computer-literate environment, except in...

...DESCRIPTORS: **Biometrics** ; ...

... **Passwords** ;

11/3,K/49 (Item 7 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01212784 SUPPLIER NUMBER: 05057242 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Variety of methods are best when plugging security holes.
Sussman, Ann
PC Week, v4, n29, p109(1)
July 21, 1987
ISSN: 0740-1604 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1278 LINE COUNT: 00104

...ABSTRACT: microcomputers and networks in corporations increases the opportunities for unauthorized access to corporate data bases. **Passwords** have long been the primary means by which users have been identified; but the US National Bureau of Standards recommends **passwords** be used along with something the user holds, such as a token with a special algorithm, and something unique to the user, such as a voice or thumb print. **Biometric** systems record such unique user traits as hand or thumb prints, retinal **eye** patterns, voice prints, or signatures. These systems often cost more than $5,000, however. Dial...

...techniques are more affordable; these systems call users back after they call in with their **passwords** . Several new security techniques are described, including challenge-response security systems and other random **password** generators.
... problem--how to ensure a user is the person he or she claims to be.
Passwords have been the traditional means of preventing unauthorized access of computer files, but they are increasingly viewed as insufficient.
" **Passwords** remain the cheapest to implement, but unless they are properly administered, they can be rendered...

...other corporate insiders have wide-ranging access to files, often including those areas in which **passwords** are stored, the static- **password** approach can't be viewed as secure, added Charles Wood, a security consultant with Information...

...Wood believes company insiders are far more likely than outsiders to breach corporate computer security. **Passwords** also are fairly easy for a wiretapper to record, he said, and "shoulder-surfing'--looking...

...s shoulder as he or she logs on--makes them easy to learn.
Recognizing the **password** 's shortcomings, the market has generated "a supermarket of solutions" to replace or complement them...

...that computer-security methods combine two of three possible features--something the user knows (a **password**); something the user holds (such as a token containing a special algorithm); and a unique...

...needs. "A blend of devices will be the best solution for some companies," she said.
Biometric systems, which are the most difficult to subvert, consist

of devices that record unique user traits such as hand or thumb prints, retinal **eye** patterns, voice prints or signatures.
Users are granted access if data transmitted from the device...

...the host computer closely approximates the user's imprint already residing there.
The cost of **biometric** systems--over $5,000 for one reader device per site on average--makes them very...

...The problem with these techniques is it's not a yes/no situation like a **password** . With **biometric** methods there are variations--your signature and voice may change," said Ms. Helsing.
Dial-back...

...systems consist of a device that sits between the modem and the host computer to **authenticate** incoming calls. A **user** at an off-site location dials the host number, inputs his or her **password** and hangs up. The protection device, which has answered the call, then dials back the...

...ground in the last two years include devices capable of generating random, one-time-only **passwords** . These include a set of hand-held products that employ " **challenge** -response" techniques to **authenticate** a **user** 's identity.
Your Algorithm, Please
In challenge-response security systems, an algorithm is included in ...

...The central computer system has the same algorithm. After logging on, the user enters a **personal identification number** into the host system. The host then sends down the "challenge," a number the user...

...to the user.
"The technique has the same effect as logging on with a different **password** each time, but you don't have to remember the **password** ," explained Linden Feldman, engineering manager of authentication products at Sytek Inc., of Mountain View, Calif...

...DESCRIPTORS: **Passwords ;**

11/3,K/50 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

02172200 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Security -- Sign On Here -- Single sign-on systems can help seal IT security while boosting worker productivity and improving enterprise management
(While no cure-all, single sign-on systems can handle diverse IT infrastructures, letting workers access everything from E-mail to high-end production applications)
Information Week, p 54
June 22, 1998
DOCUMENT TYPE: Journal; Survey ISSN: 8750-6874 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1986

(USE FORMAT 7 OR 9 FOR FULLTEXT)

ABSTRACT:
...workers access everything from E-mail to high-end production applications, using one ID and **password** . In addition to end-user

convenience, single sign-on systems can boost worker productivity by...

...a concern as client-server applications have proliferated, and the number of user IDs and **passwords** needed to access them has also risen. In a study this year by the Computer...

TEXT:
...workers access everything from E-mail to high-end production applications using one ID and **password** .

The benefits of single sign-on systems extend beyond end-user convenience. They can boost...

...logons.

As client-server applications have proliferated, so have the number of user IDs and **passwords** needed to access them. Character lengths vary, and different systems and applications carry different **password** -expiration processes. One result is that users often write down their many IDs and **passwords** and stick them on their computer monitors-despite business IT security policies that forbid this...

...the sector to achieve rapid growth, despite widespread recognition of the 'too many IDs and **passwords** ' problem," Gartner analyst Helen Flynn says in her report.

Vendors seeking to convince jaded IT...object interceptor, in which the targeted system presents its request for a user ID and **password** via a set of user interface components. The single sign-on system stores that data in an object identifier, plus the associated user ID and **password** . When the object identifier is invoked by a user attempting to log on, the **user** is **authenticated** and then the relevant **password** is plugged in to open a session. With these types of systems, IT departments don...

...link single sign-on systems with back-end systems and applications.

The addition of standard **authentication** methods such as the **Challenge** Handshake **Authentication** Protocol and others means better interoperability among the various systems. Also, most current single sign ...

...summer. The next release will support alternative authentication methods such as fingerprint readers and other **biometric** mechanisms as well as smart cards. IBM also plans to support SAP and other enterprise...

...to move beyond single sign-on to become a provider of systems that also cover **password** synchronization, security, and information access.

Others are also marketing their single sign-on software as...
...controls on a number of systems and applications, as well as synchronize user IDs and **passwords** . Control-SA doesn't reduce the number of **passwords** , but it does help an IT organization centrally manage everyone's **passwords** and access mechanisms.

Information Repository

Here's how it works: Agents are installed on the...

...to manage. These agents gather information from the system and populate a repository with the **passwords** and user IDs that are authorized to the system. For example, an NT system knows which user IDs and **passwords** are allowed to access it, and it keeps that information in a secure user

database...

...from any location. Control-SA also lets IT shops sync up the various end-user **passwords** .

Unlike native access, in which a user logs on directly to the application or system, **password** synchronization requires the end user to log on to a subsystem, such as Control-SA, which then matches that user's logon and **password** information, which is held in the repository, with all the various back-end systems the user has authority to access. "With **password** synchronization, when a **password** is changed, Control-SA will change all the other **passwords** ," Shannon says.

Companies with successful single sign-on implementations say the payback is substantial in...

...by Forrester Research Inc. suggests that as much as 80% of help-desk calls are **password** -related. Single sign-on systems could enable a company to reduce its help desk by...

11/3,K/51 (Item 1 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

07800246 (USE FORMAT 7 OR 9 FOR FULLTEXT)
BioNetrix Emerges to Deliver an Innovative User Authentication **Platform for the Internet Economy**
PR NEWSWIRE
October 18, 1999
JOURNAL CODE: WPRW LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 546

(USE FORMAT 7 OR 9 FOR FULLTEXT)
BioNetrix Emerges to Deliver an Innovative User Authentication **Platform for the Internet Economy**

...Provide a Clear, Cost-Effective Path to the Future

VIENNA, Va., Oct. 18 /PRNewswire/ -- In **response** to demand for enhanced **user verification** , BioNetrix, an **authentication** management innovator, today introduced the industry's first Authentication Management Infrastructure (AMI). By creating a standard, open platform to manage the disparate authentication technologies utilized in organizations -- **passwords** , smartcards, tokens and **biometric** solutions such as fingerprint and voice recognition -- BioNetrix is leading the AMI marketplace to allow...

... an economy where business transactions increasingly take place virtually, it is imperative for companies to **verify user** access to vital digital assets," said Peter Bianco, BioNetrix founder and CEO. "Our platform enables...

... authentication tools and can evolve with the company into the future, which we believe includes **biometrics** ."

An AMI manages end- **user verification** for multiple enterprise applications with flexible policies, using any authentication technology -- all controlled from a...

... an AMI, organizations can seamlessly and quickly migrate from weaker forms of verification, such as **passwords** , to more advanced, conclusive forms of authentication including **biometrics** . Deploying new forms of authentication is crucial in the constantly changing Internet economy.

BioNetrix was...

... and increases security in all computing environments through the deployment of superior authentication technologies -- from **passwords** , tokens and smart cards to fingerprints, facial recognition and voice verification. The company's flagship...

11/3,K/52 (Item 2 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

02495163 (USE FORMAT 7 OR 9 FOR FULLTEXT)
VASCO DATA SECURITY: Vasco Data Security announces the arrival of a newcomer to the Digipass family
M2 PRESSWIRE
August 12, 1998
JOURNAL CODE: WMPR LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 939

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... Inc. (OTC BB: VDSI) introduces the Digipass 300, an extension of its Digipass family of **user authentication** devices, or tokens. Digipass 500 and now Digipass 300 help financial institutions, companies and organisations provide secure remote access and **user authentication** to protect data. VASCO Data Security International is the only company offering a family concept...

...shipped to date.
"We have chosen the Digipass 300 because it is a modern-looking, **user** -friendly **authentication** device that we could easily integrate in our existing security infrastructure," said Harald Fatland, Project...
... authentication. To access someone's system the user needs two things: the Digipass and a **password** or **PIN** code. Without both elements, you cannot gain access to the system or network. The Digipass...

...can arise from human error."
Digipass 300: VASCO's latest innovation for secure access and **user authentication**
Provides top level **user** -friendliness The Digipass 300 represents the newest addition to the Digipass family of low-cost, **password** -protected, personal identification tools. Its high-speed optical interface allows **challenge / response authentication** , server **verification** and digital signature. 'In addition, the token supports all standard, single and triple Data Encryption...

... degree of flexibility for both security integrators and network system managers. Security parameters such as **PIN** length, number of **PIN** trials, number of host computers, type of algorithm, lengths of challenge and response are all...

...strategic objectives. From providing strong authentication technology in the form of tokens, smart cards, and **biometric** technology, to integrated authentication, access control, accounting and auditing, VASCO is at the forefront of...

11/3,K/53 (Item 1 from file: 476)
DIALOG(R)File 476:Financial Times Fulltext

0005548399 B0AJBA5ABOFT

Technology: Time to implement a security policy
DAVE MADDEN
Financial Times, P 16
Tuesday, October 2, 1990
DOCUMENT TYPE: NEWSPAPER LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
Word Count: 647

...police: open systems and electronic data interchange increase the risk.

'You can try to fix **passwords** until you are blue in the face,' says Hart, and not surprisingly, organisations are weighing the alternatives. Hart points to two routes: authentication and smart cards for basic security, and **biometric** sensors for high security systems.

Authenticators are hand-held, calculator-like devices which carry an encryption-type algorithm. After entering a **personal identification number** into a standard terminal, the user puts a computer-generated **challenge** into the **authenticator** , which calculates a **response** for the user to enter into the terminal. If the response matches what the computer
...
...the user gets access.

Smartcards use the same principle, except that the processing logic that **authenticates** the **user** is embedded in the card. **Biometric** sensors, on the other hand, identify a physical feature of the user - anything from fingerprint...

11/3,K/54 (Item 1 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2003 Business Wire. All rts. reserv.

00400660 20001102307B8025 (USE FORMAT 7 FOR FULLTEXT)
Wearable Java Computer from Dallas Semiconductor has Large, 200 Kbyte Memory for Secure Corporate Log-on and Personal Uses-New iButton with 2-in-1 Fob Speeds Smart Card Deployments with USB Reader in Handle
Business Wire
Thursday, November 2, 2000 11:13 EST
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,403

TEXT:
...public-key certificate format. In addition, the DS1957B
can store hundreds of user names and **passwords** , a color ID picture, and
the
application programs of many different service providers.

...time for applications including:

-- Access control to buildings and equipment

-- Secure network log-on using **challenge** /response **authentication**
-- Storage vault for **user** names and **passwords**

-- User profile for rapid Internet form-filling

-- Digital signatures for e-commerce

-- United States Postal...

...Security Device for PC

Postage(TM) downloadable over the Internet

-- Digital ID photo and fingerprint **biometrics**

The iButton can be updated for Web-based applications not yet invented. Because its memory...

...emerges in the marketplace, users will want to get rid of the cumbersome user name/ **password** sign-on methodology wherever possible. A much more secure method of logging onto computers is...log onto a network, sign an electronic document, safely store a list of user names/ **passwords** , keep a copy of an ID photo, and accept updates for the e-commerce transactions...

11/3,K/55 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire

0736178 BW1089

ASCEND COMMUNICATIONS: New SecureConnect From Ascend Combines IPSec Encryption and Authentication with Dynamic Firewall Protection; Combination produces the industry's most integrated and comprehensive solution for Internet-based virtual private networks

August 18, 1997

Byline: Business Editors/High Tech Writers

...scalable, secure IP connections. SecureConnect encompasses these new features and protects valuable data from prying **eyes** as it traverses the Internet."
Private Communications via the Internet
The combination of firewalls, encryption...

...SecureConnect, implemented in Ascend's MAX and Pipeline(R) families of remote networking products, include **Password** and **Challenge** -Handshake **Authentication** Protocols (PAP and CHAP); support for third-party token cards; Calling Line ID (CLID) and callback; and Network Address Translation (NAT). Access Control is Ascend's Remote **Authentication** Dial-In **User** Service (RADIUS) database solution that provides authentication, authorization and accounting management for the MAX.
"With...
?

```
?show files;ds
File 348:EUROPEAN PATENTS 1978-2003/Mar W02
         (c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20030313,UT=20030306
         (c) 2003 WIPO/Univentio

Set     Items   Description
S1       3826   (ACCESS? OR "IS()AVAILABLE" OR "MADE()AVAILABLE")(5N)(EMBE-
            D? OR ENCOD? OR FINANCIAL OR IDENTIFICATION)(3N)(CONTENT? ? OR
             DATA OR INFORMATION)
S2       2889   (CHALLENGE? OR RESPONSE)(5N)(VERIF? OR AUTHENTICAT?)
S3        235   S1 AND S2
S4         24   S1(S)S2
?t4/3,k/all

 4/3,K/1     (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2003 European Patent Office. All rts. reserv.

01320596
INFORMATION RECORDING MEDIUM, NONCONTACT IC TAG, ACCESS DEVICE, ACCESS
    SYSTEM, LIFE CYCLE MANAGEMENT SYSTEM, INPUT/OUTPUT METHOD, AND ACCESS
    METHOD
INFORMATIONSAUFZEICHNUNGSMEDIUM, TRANSPONDER, ZUGANGSEINRICHTUNG UND
    -SYSTEM, LEBENSZYKLUSVERWALTUNG, EINGANGS/AUSGANGSVERFAHREN UND
    ZUGANGSVERFAHREN
SUPPORT D'ENREGISTREMENT DE DONNEES, ETIQUETTE SANS CONTACT A CIRCUIT
    INTEGRE, DISPOSITIF D'ACCES, SYSTEME D'ACCES, SYSTEME DE GESTION DE
    CYCLE DE VIE, PROCEDE D'ENTREE/SORTIE ET PROCEDE D'ACCES
PATENT ASSIGNEE:
  MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma,
    Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
  TAMAI, Seiichiro, 18-14, Kofudai 6-chome Toyono-cho, Toyonogun Osaka
    563-0104, (JP)
  MICHISAKA, Shinichi, Room A-206 7-25, Hiyoshidai, Takatsuki-shi Osaka
    569-1022, (JP)
LEGAL REPRESENTATIVE:
  Crawford, Andrew Birkby et al (29762), A.A. Thornton & Co. 235 High
    Holborn, London WC1V 7LE, (GB)
PATENT (CC, No, Kind, Date):  EP 1205405  A1  020515 (Basic)
                              WO 200147789  010705
APPLICATION (CC, No, Date):   EP 2000987756 001226;  WO 2000JP9283  001226
PRIORITY (CC, No, Date): JP 99373880 991228; JP 200037134 000215
DESIGNATED STATES: DE; ES; FI; FR; GB; IT; NL
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: B65G-001/137; G06K-019/00; G06K-017/00;
  G06F-017/60
ABSTRACT WORD COUNT: 127
NOTE:
  Figure number on first page: 16

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS A  (English)  200220     2065
      SPEC A    (English)  200220    23205
Total word count - document A        25270
Total word count - document B            0
Total word count - documents A + B   25270

...SPECIFICATION access request instruction and the identification code,
```

the combination of the identification code and the **authenticator** **response** instruction, and the combination of the **identification** code, the **access** **information** , and the **access** instruction, from the controlling unit 102.

The instructions and operands which accompany these instructions are...

4/3,K/2 (Item 2 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01052371

Method for authentication of a mobile subscriber in a telecommunication network

Authentifizierungsverfahren fur mobile Teilnehmer in einem Telekommunikationsnetzwerk

Procede d'authentification d'abonne mobile dans un reseau de telecommunication

PATENT ASSIGNEE:

NOKIA TELECOMMUNICATIONS OY, (1268807), Keilalahdentie 4, 02150 Espoo, (FI), (applicant designated states: AT;BE;CH;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)

INVENTOR:

Purovesi, Paivi, Visakoivuntie 21 D, 02130 Espoo, (FI)

Larikka, Tapani, Riukutie 1 J 32, 00390 Helsinki, (FI)

LEGAL REPRESENTATIVE:

Cohausz & Florack (100244), Patentanwalte Kanzlerstrasse 8a, 40472 Dusseldorf, (DE)

PATENT (CC, No, Kind, Date): EP 930795 A1 990721 (Basic)

APPLICATION (CC, No, Date): EP 98100658 980116;

PRIORITY (CC, No, Date): EP 98100658 980116

DESIGNATED STATES: BE; DE; FI; FR; GB; IT; NL; SE

INTERNATIONAL PATENT CLASS: H04Q-007/38; H04Q-007/24;

ABSTRACT WORD COUNT: 144

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9929	883
SPEC A	(English)	9929	2248
Total word count - document A			3131
Total word count - document B			0
Total word count - documents A + B			3131

...CLAIMS which the Mobile Switching Centre (MSC) requests authentication data of the mobile subscriber

- transmitting an **AUTHENTICATION** **RESPONSE** message from Mobile Station (MS) to Mobile Switching Centre (MSC) via **Access** Network (AN), which comprises secret **encoded** authentication **data** (SRES) of the subscriber

- transmitting an IDENTITY REQUEST message from Mobile Switching Centre (MSC) to...

...transmitting an IDENTITY RESPONSE message from Mobile Station (MS) to Mobile Switching Centre (MSC) via **Access** Network (AN), which comprises the **identification** **data** (IMSI) of the subscriber

- determining by Mobile Switching Centre (MSC) whether received encoded authentication data...

...via Access Network (AN) to enable the internal call in case of corresponding of received **encoded** authentication **data** and expected **encoded** authentication **data**

- **Access** Network (AN) terminates connection with Mobile Switching Centre (MSC)
- continuing with internal service connection
- transmitting rejection signal from Mobile Switching Centre (MSC) to Mobile Station (MS) via **Access** Network (AN) in case the received **encoded** authentication **data** does not correspond to the expected encoded authentication data
- terminating all transactions

3. Method according...

4/3,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00957813
PERSONAL ELECTRONIC SETTLEMENT SYSTEM, ITS TERMINAL, AND MANAGEMENT APPARATUS
PERSONLICHES ELEKTRONISCHES REGELUNGSSYSTEM, TERMINAL UND MANAGEMENTAPPARAT
SYSTEME DE REGLEMENT ELECTRONIQUE PERSONNEL, TERMINAL DE CE DERNIER ET APPAREIL PERMETTANT DE GERER CE SYSTEME
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza Kadoma, Kadoma-shi, Osaka-fu, 571, (JP), (applicant designated states: DE;FR;GB)
INVENTOR:
TAKAYAMA, Hisashi, 21-22, Matsubara 4-chome,Setagaya-ku, Tokyo 156, (JP)
LEGAL REPRESENTATIVE:
Casalonga, Axel et al (14511), BUREAU D.A. CASALONGA - JOSSE Morassistrasse 8, 80469 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 910028 A1 990421 (Basic)
WO 9821677 980522
APPLICATION (CC, No, Date): EP 97912468 971114; WO 97JP4161 971114
PRIORITY (CC, No, Date): JP 96316897 961114; JP 97117681 970422
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: G06F-017/60;
ABSTRACT WORD COUNT: 119

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9916	12261
SPEC A	(English)	9916	116678
Total word count - document A			128939
Total word count - document B			0
Total word count - documents A + B			128939

...SPECIFICATION and the person in charge thereof, specifies the first service providing means by employing the **identification information** , for the charging means, that is stored in the second storage means of the second...

4/3,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00921020
Optical disc system having current monitoring circuit with controller for laser driver and method for operating same
Optisches Plattensystem mit Stromuberwachungsschaltung mit Lasertreibersteuerungseinheit, und Verfahren zu deren Betrieb

Systeme de disque optique avec circuit de surveillance de courant avec dispositif de commande d'un laser, et methode de fonctionnement

PATENT ASSIGNEE:
DISCOVISION ASSOCIATES, (260273), 2355 Main Street Suite 200, Irvine, CA 92714, (US), (applicant designated states: AT;BE;CH;DE;ES;FR;GB;IE;IT;LI;NL;PT;SE)

INVENTOR:
Crupper, Randolph Scott, 308 High Street, PO Box 731, Palmer Lake, Colorado 80133, (US)
Davis, Marvin Benjamin, 2813 Palmer Park Blvd., Colorado Springs, Colorado 80909, (US)
Getreuer, Kurt Walter, 115 Golden Hills Rd., Colorado Springs, Colorado 80919, (US)
Grassens, Leonardus Johannes, 19115 Pebble Beach Way, Monument, Colorado 80132, (US)
Lewis, David Earl, 14820 Spiritwood Loop, Black Forest, Colorado 80106, (US)
Schell, David Louis, 5307 Borrego Drive, Colorado Springs, Colorado 80918, (US)

LEGAL REPRESENTATIVE:
Bazzichelli, Alfredo et al (40161), c/o Societa Italiana Brevetti S.p.A. Piazza di Pietra, 39, 00186 Roma, (IT)

PATENT (CC, No, Kind, Date): EP 840309 A2 980506 (Basic)
EP 840309 A3 990414
APPLICATION (CC, No, Date): EP 97118099 960118;
PRIORITY (CC, No, Date): US 376882 950125
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; IE; IT; LI; NL; PT; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 726564 (EP 963003504)
INTERNATIONAL PATENT CLASS: G11B-011/10; G11B-007/09;
ABSTRACT WORD COUNT: 115

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9819	2633
SPEC A	(English)	9819	88350
Total word count - document A			90983
Total word count - document B			0
Total word count - documents A + B			90983

...SPECIFICATION respective medium, data encoding means being responsive to the data receiving means for representing the **data** to be stored in a predetermined format, the **data encoding** means also for directing **data** to the third electronic means, write means, coacting with the third electronic means, for writing...

4/3,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00921019
Isolation apparatus for use in disc drive system to mitigate effects of undesired mechanical forces and disc drive system including same
Isolierungsvorrichtung zur Verwendung in einem Plattenantriebssystem zur Verminderung der Effekte von ungewunschten mechanischen Kraften, und Plattenantriebssys
Appareil d'isolation utilisable dans un systeme d'entrainement de disque pour mitiger les effets des forces mecaniques indesirables, et systeme d'entrainement p
PATENT ASSIGNEE:

DISCOVISION ASSOCIATES, (260273), 2355 Main Street Suite 200, Irvine, CA 92714, (US), (applicant designated states: AT;BE;CH;DE;ES;FR;GB;IE;IT;LI;NL;PT;SE)
INVENTOR:
Crupper, Randolph Scott, 308 High Street, PO Box 731, Palmer Lake, Colorado 80133, (US)
Davis, Marvin Benjamin, 2813 Palmer Park Blvd., Colorado Springs, Colorado 80909, (US)
Getreuer, Kurt Walter, 115 Golden Hills Rd., Colorado Springs, Colorado 80919, (US)
Grassens, Leonardus Johannes, 19115 Pebble Beach Way, Monument, Colorado 80132, (US)
Lewis, David Earl, 14820 Spiritwood Loop, Black Forest, Colorado 80106, (US)
Schell, David Louis, 5307 Borrego Drive, Colorado Springs, Colorado 80918 , (US)
LEGAL REPRESENTATIVE:
Bazzichelli, Alfredo et al (40161), c/o Societa Italiana Brevetti S.p.A. Piazza di Pietra, 39, 00186 Roma, (IT)
PATENT (CC, No, Kind, Date): EP 840301 A2 980506 (Basic)
EP 840301 A3 990414
APPLICATION (CC, No, Date): EP 97118096 960118;
PRIORITY (CC, No, Date): US 376882 950125
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; IE; IT; LI; NL; PT; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 726564 (EP 963003504)
INTERNATIONAL PATENT CLASS: G11B-007/085; G11B-007/09; G11B-011/10; G11B-033/08;
ABSTRACT WORD COUNT: 79

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9819	6554
SPEC A	(English)	9819	88292
Total word count - document A			94846
Total word count - document B			0
Total word count - documents A + B			94846

...SPECIFICATION respective medium, data encoding means being responsive to the data receiving means for representing the **data** to be stored in a predetermined format, the **data encoding** means also for directing **data** to the third electronic means, write means, coacting with the third electronic means, for writing...

4/3,K/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2003 European Patent Office. All rts. reserv.

00671707
A method for utilising medium nonuniformities to minimize unauthorized duplication of digital information
Verfahren zur Verwendung von Mediuminhomogenitaten zur Minimierung unbefugter Vervielfaltigung digitaler Daten
Methode pour reduire au minimum la duplication non-autorisee de donnees digitales en utilisant des non-uniformites d'un support de memoire
PATENT ASSIGNEE:
NATIONAL UNIVERSITY OF SINGAPORE, (1216932), Heng Mui Keng Terrace, Kent Ridge, Singapore 0511, (SG), (applicant designated states: DE;GB)
INVENTOR:
Arcot Desai, Narasimhalu, 9 Ross Avenue, Singapore 1129, (SG)

Wang, Weiguo, 103 Jalan Hitam Manis, Singapore 1027, (SG)
Kankanhalli, Mohan Shankara, 74 Jalan Hitam Manis, Singapore 1027, (SG)
LEGAL REPRESENTATIVE:
Driver, Virginia Rozanne et al (58902), Page White & Farrer 54 Doughty Street, London WC1N 2LS, (GB)
PATENT (CC, No, Kind, Date): EP 644474 A1 950322 (Basic)
EP 644474 B1 980805
APPLICATION (CC, No, Date): EP 94306679 940912;
PRIORITY (CC, No, Date): US 120969 930913
DESIGNATED STATES: DE; GB
INTERNATIONAL PATENT CLASS: G06F-001/00; G11B-020/00;
ABSTRACT WORD COUNT: 227

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9832	329
CLAIMS B	(German)	9832	312
CLAIMS B	(French)	9832	349
SPEC B	(English)	9832	3692
Total word count - document A			0
Total word count - document B			4682
Total word count - documents A + B			4682

...CLAIMS by the device.
2. A method according to claim 1 wherein the device for which **access** to the **information** is permitted has a device **identification** (ID) and wherein:

in step b), the device identification (ID) is also incorporated (100) into...
...encryption key; in step c), access to the storage medium by the device is in **response** to **verification** (170, 200) of the signature and the device identification (ID) of the device; and in...

4/3,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2003 European Patent Office. All rts. reserv.

00513290
System for integrating telephony data with data processing systems.
System zur Integrierung von Telefondaten in einem Datenverarbeitungssystem.
Systeme pour integrer des donnees telephoniques dans des systemes de traitement de donnees.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB)
INVENTOR:
Gursahaney, Suresh K., 18761 Nathan's Place, Gaithersburg, MD 20879, (US)
Helm, Daniel J., 1200 Buchanan Street, McLean, VA 22101, (US)
Lee, Dana R., 9095 Manorwood Road, Laurel, MD 20723, (US)
Madrid, Richard J., 66 West Deer Park Road, Apt. 202, Gaithersburg, MD 20877, (US)
McKenzie, Valerie S., 3935 E. 177 Street, Cleveland, Ohio 44128, (US)
Miller, Steven K., 20721 Burnt Woods Drive,, Germantown, MD 20874, (US)
LEGAL REPRESENTATIVE:
Teufel, Fritz, Dipl.-Phys. et al (11855), IBM Deutschland Informationssysteme GmbH, Patentwesen und Urheberrecht, 70548 Stuttgart , (DE)
PATENT (CC, No, Kind, Date): EP 501189 A2 920902 (Basic)
EP 501189 A3 931118

APPLICATION (CC, No, Date): EP 92101849 920205;
PRIORITY (CC, No, Date): US 660763 910225
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: G06F-009/46;
ABSTRACT WORD COUNT: 74

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	2343
SPEC A	(English)	EPABF1	12756
Total word count - document A			15099
Total word count - document B			0
Total word count - documents A + B			15099

...CLAIMS menu buffered in said first window, using a verify means in said interface program in **response** to a **verify** command in said host **access** table;

inserting an operand derived from the caller **identification data** received from said telephone network into a predefined location in said first menu buffered in...

4/3,K/8 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00984068 **Image available**
PRINTING CARTRIDGE WITH RADIO FREQUENCY IDENTIFICATION
CARTOUCHE D'IMPRESSION AVEC IDENTIFICATION PAR RADIOFREQUENCE
Patent Applicant/Assignee:
SILVERBROOK RESEARCH PTY LTD, 393 Darling Street, Balmain, New South Wales 2041, AU, AU (Residence), AU (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
SILVERBROOK KIA, Silverbrook Research Pty Ltd, 393 Darling Street, Balmain, New South Wales 2041, AU, AU (Residence), AU (Nationality), (Designated only for: US)
Legal Representative:
SILVERBROOK KIA (agent), Silverbrook Research Pty Ltd, 393 Darling Street, Balmain, New South Wales 2041, AU,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200313864 A1 20030220 (WO 0313864)
Application: WO 2002AU913 20020709 (PCT/WO AU0200913)
Priority Application: US 2001922047 20010806
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 141831

Fulltext Availability:
Detailed Description

Detailed Description

... thus becomes a black line with white on either side, making for a good frequency **response** on reading. The clockmark-s alternating between white and black have a similar result, except...to the alternative Artcard, the entire data is completely recoverable, even if there is no **data** duplication.

Write the scrambled **encoded** **data** to the alternative Artcard
Once the original **data** has been Reed-Solomon **encoded** , duplicated, and scrambled, there are 1,827,840 bytes of data to be stored on...

4/3,K/9 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00981068 **Image available**
METHOD AND SYSTEM FOR DATA MANAGEMENT IN ELECTRONIC PAYMENTS TRANSACTIONS
PROCEDE ET SYSTEME DE GESTION DE DONNEES DANS DES TRANSACTIONS A PAIEMENTS ELECTRONIQUES
Patent Applicant/Assignee:
CITIBANK N A, 909 Third Avenue, 28th Floor, New York, NY 10022, US, US (Residence), US (Nationality)
Inventor(s):
NAGY Dan, 36 Fairway Place, Cold Spring Harbor, NY 11724, US,
GOOTT Paul, 318 Main Street, #33, Madison, NJ 07940, US,
LANDRY John, 54 Center Avenue Extension, Norwalk, CT 06851, US,
COX David, 49 Harding Road, Old Greenwich, CT 06870, US,
PANG Michael C, 239-36 66th Avenue, Douglaston, NY 11362, US,
FAVOLE Joe, 20 Cherry Lane, Howell, NJ 07731, US,
THOMPSON Michael, 104 Woodview Lane, Centereach, NY 11720, US,
Legal Representative:
MARCOU George (agent), Kilpatrick Stockton LLP, 607 Fourteenth St., N.W., Suite 900, Washington, DC 20005, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200310951 A1 20030206 (WO 0310951)
Application: WO 2002US23099 20020722 (PCT/WO US0223099)
Priority Application: US 2001307525 20010724
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 14246

Fulltext Availability:
Detailed Description
Claims

Detailed Description
... the invention, the mobile payments engine receives the user's entry via an interactive voice **response** unit of user identity **verification** and **financial** source account **information** that allows the mobile payments engine **access** to at least one source account of funds of the user through
a link. The...

Claim

... a mobile payments engine adapted for receiving a user's entry via an interactive voice **response** unit of user identification **verification** and **financial** source account **information** that allows the mobile payments engine **access** to

4/3,K/10 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00979516 **Image available**
METHOD AND SYSTEM FOR USER AND GROUP AUTHENTICATION WITH PSEUDO-ANONYMITY OVER A PUBLIC NETWORK
PROCEDE ET SYSTEME D'AUTHENTIFICATION D'UN UTILISATEUR OU D'UN GROUPE DE FACON PSEUDO-ANONYME SUR UN RESEAU PUBLIC
Patent Applicant/Assignee:
WAVE SYSTEMS CORP, 480 Pleasant Street, Lee, MA 01238, US, US (Residence), US (Nationality)
Inventor(s):
SPRAGUE Steven, 147 Reservoir Road, Lenox, MA 01240, US,
Legal Representative:
BUTTER Gary M (agent), Baker & Botts LLP, 30 Rockefeller Plaza, New York, NY 10112-4498, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200309511 A1 20030130 (WO 0309511)
Application: WO 2002US21633 20020710 (PCT/WO US0221633)
Priority Application: US 2001906375 20010716
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 5720

Fulltext Availability:
Detailed Description

Detailed Description
... associates the identifier of the persona or group with a publisher identification and a database **identification** which are pointers to a **data** set **access** record stored in one of the digital rights management (DRM) server 202 or account manager...which are used by the DRM server 202 to encrypt the random number of the **challenge** message to generate the **authentication** object which is passed from the DRM server 202 to the authentication server 200 (step...

...200 can correlate the authentication object with the persona or group identifier provided in the **challenge** message and provide the **authentication** object to the content provider computer (step 430).

Figure 5 is a simplified flow chart...

4/3,K/11 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00852800 **Image available**

DYNAMIC DISPLAY OBJECTS IN A DISTRIBUTED COMPUTING ENVIRONMENT
AFFICHAGES DYNAMIQUES DANS UN ENVIRONNEMENT D'INFORMATIQUE DISTRIBUEE

Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 901 San Antonio Road, Palo Alto, CA 94303, US, US (Residence), US (Nationality)
Inventor(s):
SLAUGHTER Gregory L, 3326 Emerson Street, Palo Alto, CA 94306, US,
SAULPAUGH Thomas E, 6938 Bret Harte Drive, San Jose, CA 95120, US,
TRAVERSAT Bernard A, Apartment 402, 2055 California Street, San Francisco, CA 94109, US,
ABDELAZIZ Mohamed M, 78 Cabot Avenue, Santa Clara, CA 95051, US,
Legal Representative:
KOWERT Robert C (agent), Conley, Rose & Tayon, P.C., P.O. Box 398, Austin, TX 78767-0398, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200186424 A2-A3 20011115 (WO 0186424)
Application: WO 2001US15137 20010509 (PCT/WO US0115137)
Priority Application: US 2000202975 20000509; US 2000208011 20000526; US 2000209430 20000602; US 2000209140 20000602; US 2000209525 20000605; US 2000693321 20001019
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 73634

Fulltext Availability:
Detailed Description

Detailed Description
... resuits data produced for the client by the service. The presentation schema may include fonnatting, **data** type, and other **information** for use in presenting resuits **data** produced by the service. In one embodiment, the client may use a display service to...A client may obtain an authentication credential. In one embodiment, the space may provide an **authentication** service in **response** to a client's request for access to the space. The client may obtain the...embodiment, these checks may be implemented using access control lists (ACLs) in conjunction with an **authentication** service such as Kerberos. A **challenge** -response sequence 65
(such as a password) may also be used to authenticate a client...y the client as a valid client. In one embodiment, the client may access the **authentication** service using a **challenge / response** mechanism such as a logon account with password and thus may be verified as a...

...the security checks may be implemented using Access Control Lists (ACLs) in conjunction with an **authentication** service. In one embodiment, a **challenge** /response sequence (such as a logon and password account) may be used to authenticate a...some or all of the request message verification prior to sending request messages and the **response** message **verification** subsequent to receiving **response** messages as described above. For example; some simple client devices may include a small set...

...message gate may be constructed for the client device that sends request messages and receives **response** messages without perfonning the message

verification as described above. In another embodiment, a proxy client message gate may be set up...

4/3,K/12 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00840300 **Image available**
OPERATIONS AND MAINTENANCE ARCHITECTURE FOR MULTIPROTOCOL DISTRIBUTED SYSTEM
OPERATIONS ET ARCHITECTURE DE MAINTENANCE POUR SYSTEME DISTRIBUE MULTIPROTOCOLE
Patent Applicant/Assignee:
TRANSCEPT OPENCELL INC, 955 Perimeter Road, Manchester, NH 03103, US, US (Residence), US (Nationality)
Inventor(s):
SABAT John Jr, 16 Hansom Drive, Merrimack, NH 03054, US,
MILLAR Jeffrey R, 37 Springs Hill Road, Mont Vernon, NH 03057, US,
Legal Representative:
THIBODEAU David J Jr (et al) (agent), Hamilton, Brook, Smith & Reynolds, P.C., 530 Virginia Road, P.O. Box 9133, Concord, MA 01742-9133, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200174013 A2-A3 20011004 (WO 0174013)
Application: WO 2001US40394 20010329 (PCT/WO US0140394)
Priority Application: US 2000192870 20000329; US 2001821820 20010329
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7230

Fulltext Availability:
Detailed Description

Detailed Description
... IP address of originating
authorized tenant NMS 62;
6. The SNMP agent in the open **access** NMS 60 uses the Tenant **identification information** and SNMP address to look up the validity of message in a local
MEB copy...

...open access statefall firewall NMS 60;
9. The open access statefiall firewall NMS 60 receives **response** and **verifies** its
association with an SNMP message; it may also verifies the origin and destination IP...

4/3,K/13 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00831853 **Image available**
USE OF INTERNET SITE AS A REGISTRY FOR RESULTS OF MEDICAL TESTS

UTILISATION DE SITE INTERNET COMME SITE D'ENREGISTREMENT DE RESULTATS DE TESTS MEDICAUX
Patent Applicant/Inventor:
DEMOPULOS Gregory, 6530 83rd Place S.E., Mercer Island, WA 98040, US, US (Residence), US (Nationality)
Legal Representative:
ANDERSON Ronald (agent), Law Offices of Ronald M. Anderson, 600 108th Avenue NE, Suite 507, Bellevue, WA 98004, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200165443 A1 20010907 (WO 0165443)
Application: WO 2001US5662 20010223 (PCT/WO US0105662)
Priority Application: US 2000185562 20000228; US 2000566530 20000508
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 12730

Fulltext Availability:
Claims

Claim
... subscriber identification data. Optionally, such customer ID can be verified by the testing lab by **accessing** the registry site. Although various types of **identification data** are contemplated, the simplest verification data for the subscriber's identification is the driver's... or her customer ID and password, thereby accessing the partner subscriber's testing history and **verifying** that the automated **response** previously heard was, indeed, generated by the registry site and was not a fraudulent automated...

4/3,K/14 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00823039
NUCLEIC ACIDS, PROTEINS, AND ANTIBODIES
ACIDES NUCLEIQUES, PROTEINES ET ANTICORPS
Patent Applicant/Assignee:
HUMAN GENOME SCIENCES INC, 9410 Key West Avenue, Rockville, MD 20850, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
ROSEN Craig A, 22400 Rolling Hill Lane, Laytonsville, MD 20882, US, US (Residence), US (Nationality), (Designated only for: US)
BARASH Steven C, 111 Watkins Pond Blvd. #301, Rockville, MD 20850, US, US (Residence), US (Nationality), (Designated only for: US)
RUBEN Steven M, 18528 Heritage Hills Drive, Olney, MD 20832, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
HOOVER Kenley K (et al) (agent), Human Genome Sciences, Inc., 9410 Key West Avenue, Rockville, MD 20850, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200155355 A1 20010802 (WO 0155355)
Application: WO 2001US1351 20010117 (PCT/WO US0101351)

Priority Application: US 2000179065 20000131; US 2000180628 20000204; US 2000184664 20000224; US 2000186350 20000302; US 2000189874 20000316; US 2000190076 20000317; US 2000198123 20000418; US 2000205515 20000519; US 2000209467 20000607; US 2000214886 20000628; US 2000215135 20000630; US 2000216647 20000707; US 2000216880 20000707; US 2000217487 20000711; US 2000217496 20000711; US 2000218290 20000714; US 2000220963 20000726; US 2000220964 20000726; US 2000225757 20000814; US 2000225270 20000814; US 2000225447 20000814; US 2000225267 20000814; US 2000225758 20000814; US 2000225268 20000814; US 2000224518 20000814; US 2000224519 20000814; US 2000225759 20000814; US 2000225213 20000814; US 2000225266 20000814; US 2000225214 20000814; US 2000226279 20000818; US 2000226868 20000822; US 2000227182 20000822; US 2000226681 20000822; US 2000227009 20000823; US 2000228924 20000830; US 2000229344 20000901; US 2000229343 20000901; US 2000229287 20000901; US 2000229345 20000901; US 2000229513 20000905; US 2000229509 20000905; US 2000230438 20000906; US 2000230437 20000906; US 2000231413 20000908; US 2000232080 20000908; US 2000231414 20000908; US 2000231244 20000908; US 2000232081 20000908; US 2000231242 20000908; US 2000231243 20000908; US 2000231968 20000912; US 2000232401 20000914; US 2000232399 20000914; US 2000232400 20000914; US 2000232397 20000914; US 2000233063 20000914; US 2000233064 20000914; US 2000233065 20000914; US 2000232398 20000914; US 2000234223 20000921; US 2000234274 20000921; US 2000234997 20000925; US 2000234998 20000925; US 2000235484 20000926; US 2000235834 20000927; US 2000235836 20000927; US 2000236369 20000929; US 2000236327 20000929; US 2000236370 20000929; US 2000236368 20000929; US 2000236367 20000929; US 2000237039 20001002; US 2000237038 20001002; US 2000237040 20001002; US 2000237037 20001002; US 2000236802 20001002; US 2000239937 20001013; US 2000239935 20001013; US 2000241785 20001020; US 2000241809 20001020; US 2000240960 20001020; US 2000241787 20001020; US 2000241808 20001020; US 2000241221 20001020; US 2000241786 20001020; US 2000241826 20001020; US 2000244617 20001101; US 2000246474 20001108; US 2000246532 20001108; US 2000246476 20001108; US 2000246526 20001108; US 2000246475 20001108; US 2000246525 20001108; US 2000246528 20001108; US 2000246527 20001108; US 2000246477 20001108; US 2000246611 20001108; US 2000246610 20001108; US 2000246613 20001108; US 2000246609 20001108; US 2000246478 20001108; US 2000246524 20001108; US 2000246523 20001108; US 2000249299 20001117; US 2000249210 20001117; US 2000249216 20001117; US 2000249217 20001117; US 2000249211 20001117; US 2000249215 20001117; US 2000249218 20001117; US 2000249208 20001117; US 2000249213 20001117; US 2000249212 20001117; US 2000249207 20001117; US 2000249245 20001117; US 2000249244 20001117; US 2000249297 20001117; US 2000249214 20001117; US 2000249264 20001117; US 2000249209 20001117; US 2000249300 20001117; US 2000249265 20001117; US 2000250391 20001201; US 2000250160 20001201; US 2000256719 20001205; US 2000251030 20001205; US 2000251988 20001205; US 2000251479 20001206; US 2000251869 20001208; US 2000251856 20001208; US 2000251868 20001208; US 2000251990 20001208; US 2000251989 20001208; US 2000254097 20001211; US 2001259678 20010105

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English
Filing Language: English
Fulltext Word Count: 170529

Fulltext Availability:
Detailed Description

Detailed Description

... sequences of SEQ ID NOX
63
[0531 The predicted amino acid sequence can then be **verified** from such deposits.
Moreover, the amino acid sequence of the protein encoded by a particular ...polypeptide of SEQ ID NOX; is a polynucleotide sequence encoding a portion of a polypeptide **encoded** by SEQ ID NOA; is a polynucleotide sequence **encoding** a portion of a polypeptide **encoded** by the complement of the polynucleotide sequence in SEQ ID NOA; is a portion of ...

4/3,K/15 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00806382
METHOD FOR AFFORDING A MARKET SPACE INTERFACE BETWEEN A PLURALITY OF MANUFACTURERS AND SERVICE PROVIDERS AND INSTALLATION MANAGEMENT VIA A MARKET SPACE INTERFACE
PROCEDE DE MISE A DISPOSITION D'UNE INTERFACE D'ESPACE DE MARCHE ENTRE UNE PLURALITE DE FABRICANTS ET DES FOURNISSEURS DE SERVICES ET GESTION D'UNE INSTALLATION VIA UNE INTERFACE D'ESPACE DE MARCHE
Patent Applicant/Assignee:
ACCENTURE LLP, 1661 Page Mill Road, Palo Alto, CA 94304, US, US (Residence), US (Nationality)
Inventor(s):
MIKURAK Michael G, 108 Englewood Blvd., Hamilton, NJ 08610, US,
Legal Representative:
HICKMAN Paul L (et al) (agent), Oppenheimer Wolff & Donnelly LLP, 1400 Page Mill Road, Palo Alto, CA 94304, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200139028 A2 20010531 (WO 0139028)
Application: WO 2000US32308 20001122 (PCT/WO US0032308)
Priority Application: US 99444773 19991122; US 99444798 19991122
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 170977

Fulltext Availability:
Detailed Description

Detailed Description
... The WorldWide Web is a collection of servers connected to the Internet that provide multimedia **information** to users that request the **information** . The users **access** the information using client programs called "browsers" to display the multi-media information.

known as...sale" price reverts to the "regular" price. If a merchant wishes to change prices in **response** to a competitor's price, usually special effort
174
is required to change price tags...retrieving the article to provide the article to the article pickup area upon obtaining the **identification**

information and comparing the **identification** with the customer's purchase order.

The present invention also encompasses a method for ordering...

4/3,K/16 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00794377 **Image available**
SYSTEM AND METHOD FOR GLOBAL INTERNET DIGITAL IDENTIFICATION
SYSTEME ET PROCEDE D'IDENTIFICATION NUMERIQUE GLOBALE SUR INTERNET
Patent Applicant/Assignee:
MASTERCARD INTERNATIONAL INCORPORATED, 2000 Purchase Street, Purchase, NY 10577-2509, US, US (Residence), US (Nationality)
Inventor(s):
HARRIS Michael D S, 1521 Pennsylvania Avenue, Paoli, PA 19301, US,
WANKMUELLER John, 11 Evergreen Lane, New Hyde Park, NY 11040, US,
Legal Representative:
SCHEINFELD Robert S (et al) (agent), Baker & Botts, LLP, 30 Rockefeller Plaza, New York, NY 10112-0228, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200127887 A1 20010419 (WO 0127887)
Application: WO 2000US27458 20001005 (PCT/WO US0027458)
Priority Application: US 99158608 19991008; US 99163886 19991105
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 6637

Fulltext Availability:
Claims

Claim
... holder; the authorization response message includes a password suitable for enabling
the ID holder to **access** a web site;
the **identification data** includes at least one of a payment amount field and a
validation level amount field...

...data related to at least one of the identification data, the authorization request message, the **authentication** operation, the authorization **response** message, and the output response message, said transaction data including
said transaction certificate;
incorporating the...

4/3,K/17 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00784125

SYSTEM, METHOD, AND ARTICLE OF MANUFACTURE FOR PIECEMEAL RETRIEVAL IN AN INFORMATION SERVICES PATTERNS ENVIRONMENT
SYSTEME, PROCEDE ET ARTICLE DE FABRICATION DESTINES A LA RECHERCHE FRAGMENTAIRE DANS UN ENVIRONNEMENT DE MODELES DE SERVICES D'INFORMATIONS
Patent Applicant/Assignee:
ACCENTURE LLP, 1661 Page Mill Road, Palo Alto, CA 94304, US, US (Residence), US (Nationality)
Inventor(s):
BOWMAN-AMUAH Michel K, 6426 Peak Vista Circle, Colorado Springs, CO 80918, US,
Legal Representative:
HICKMAN Paul L (agent), Oppenheimer Wolff & Donnelly, LLP, 38th Floor, 2029 Century Park East, Los Angeles, CA 90067-3024, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200116705 A2-A3 20010308 (WO 0116705)
Application: WO 2000US24085 20000831 (PCT/WO US0024085)
Priority Application: US 99386433 19990831
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 150355

Fulltext Availability:
Detailed Description

Detailed Description
... 48 illustrates the Enterprise Information Architecture (EIA) model; Figure 49 illustrates a V-model of **Verification** , Validation, and Testing; Figure 50 portrays of a development architecture with a seamless integration of...other vendors?
Delivery schedule to provide adequate pre-conversion testing?
Backup procedures?
Vendor reliability and **financial** stability?
Future proofing against business change?
Have the versions of system software been live at...

4/3,K/18 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00777021
A SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR AN E-COMMERCE BASED USER FRAMEWORK DESIGN FOR MAINTAINING USER PREFERENCES, ROLES AND DETAILS
SYSTEME, PROCEDE ET ARTICLE MANUFACTURE UTILISES EN COMMERCE ELECTRONIQUE POUR LA CONCEPTION DE STRUCTURES D'UTILISATEURS DESTINEES A PRESERVER LES PREFERENCES, ROLES ET DETAILS DES UTILISATEURS
Patent Applicant/Assignee:
ACCENTURE LLP, Parkstraat 83, NL-2514 JG 's Gravenhage, The Hague, NL, NL (Residence), NL (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
UNDERWOOD Roy A, 4436 Hearthmoor Court, Long Grove, IL 60047, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:

HICKMAN Paul L (agent), Oppenheimer Wolff & Donnelly LLP, 1400 Page Mill Road, Palo Alto, CA 94304, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200109792 A2-A3 20010208 (WO 0109792)
Application: WO 2000US20549 20000728 (PCT/WO US0020549)
Priority Application: US 99364091 19990730
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 122232

Fulltext Availability:
Detailed Description

Detailed Description
... Security through the ReTA Session and Activity frameworks.

The Session framework provides "Session level Page **access** authorization", "User **identification** " and "session timeout" services. The Activity framework provides "Activity level Page access authorization".

Codes Table...probably
because
'the Session timed-out and so display the timeout message
if theCurrentPage = "/asp/ **verifpwd** .asp" then
'do nothing
else
response .Redirect("/asp/ExamplePages/timeout.htm")
endif
endif
Here are some of the basic technologies utilized...Distributed Password Authentication (DPA)
DPA works for Membership authentication in much the same way as **Challenge / Response** works for Windows NT **Authentication** . For DPA, users are authenticated against the Membership Directory (rather than the Windows NT SAM...

...be selected simultaneously. In this case, the server may first attempt to issue a DPA **authentication challenge** . If (and only if) the client cannot interpret the challenge, the server may offer the...

4/3,K/19 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00777020
A SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR RESOURCE ADMINISTRATION IN AN E-COMMERCE TECHNICAL ARCHITECTURE
SYSTEME, PROCEDE ET ARTICLE MANUFACTURE POUR L'ADMINISTRATION DE RESSOURCES DANS UNE ARCHITECTURE TECHNIQUE DE COMMERCE ELECTRONIQUE
Patent Applicant/Assignee:
ACCENTURE LLP, Parkstraat 83, NL-2514 JG 'S Gravenhage, NL, NL (Residence), NL (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:
UNDERWOOD Roy A, 4436 Hearthmoor Court, Long Grove, IL 60047, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
HICKMAN Paul L (agent), Oppenheimer Wolff & Donnelly, LLP, P.O. Box 52037, Palo Alto, CA 94303-0746, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200109791 A2-A3 20010208 (WO 0109791)
Application: WO 2000US20547 20000728 (PCT/WO US0020547)
Priority Application: US 99364161 19990730
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 136396

Fulltext Availability:
Detailed Description

Detailed Description
... of the present descriptions no matter where they are located, through the use of links **embedded** into the portion of the present description **content** . Web Browser Services retain the link connection, i.e., portion of the present description physical...

4/3,K/20 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00777012
A SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR PROVIDING AN INTERFACE BETWEEN A FIRST SERVER AND A SECOND SERVER.
SYSTEME, PROCEDE ET ARTICLE MANUFACTURE DESTINES A UNE ARCHITECTURE DE COMMERCE ELECTRONIQUE BASEE SUR JAVA
Patent Applicant/Assignee:
ACCENTURE LLP, 1661 Page Mill Road, Palo Alto, CA 94304, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
UNDERWOOD Roy A, 4436 Hearthmoor Court, Long Grove, IL 60047, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
HICKMAN Paul L (agent), Oppenheimer Wolff & Donnelly, LLP, 38th floor, 2029 Century Park East, Los Angeles, CA 90067-3024, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200109721 A2-A3 20010208 (WO 0109721)
Application: WO 2000US20561 20000728 (PCT/WO US0020561)
Priority Application: US 99364531 19990730
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English
Filing Language: English
Fulltext Word Count: 126924

Fulltext Availability:
Detailed Description

Detailed Description
... Frameworks require the tables and relationships illustrated in Figure 54. Among these tables are user **identification** tables 5400, user preference tables 5402, and event log tables 5404.

Application Tables
Figure 55...probably
because
'the Session timed-out and so display the timeout message
if theCurrentPage = "/asp/ **verifpwd** .asp" then
'do nothing
else
response .Redirect("/asp/ExamplePages/timeout.htm")
endif
endif
Here are some of the basic technologies utilized...Distributed Password Authentication (DPA)
DPA works for Membership authentication in much the same way as **Challenge / Response** works for Windows NT **Authentication** . For DPA, users are authenticated against the Membership Directory (rather than the Windows NT SAM...

...be selected simultaneously. In this case, the server may first attempt to issue a DPA **authentication challenge** . If (and only if) the client cannot interpret the challenge, the server may offer the...

4/3,K/21 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00744485
48 HUMAN SECRETED PROTEINS
48 PROTEINES HUMAINES SECRETEES
Patent Applicant/Assignee:
HUMAN GENOME SCIENCES INC, 9410 Key West Avenue, Rockville, MD 20850, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
ROSEN Craig A, 22400 Rolling Hill Road, Laytonsville, MD 20882, US, US (Residence), US (Nationality), (Designated only for: US)
RUBEN Steven M, 18528 Heritage Hills Drive, Laytonsville, MD 20882, US, US (Residence), US (Nationality), (Designated only for: US)
KOMATSOULIS George, 9518 Garwood Street, Silver Spring, MD 20901, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
HOOVER Kenley K, Human Genome Sciences, Inc., 9410 Key West Avenue, Rockville, MD 20850, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200056765 A1 20000928 (WO 0056765)
Application: WO 2000US6823 20000316 (PCT/WO US0006823)
Priority Application: US 99125364 19990319; US 99169623 19991208
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ

TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 129608

Fulltext Availability:
Detailed Description

Detailed Description
... a non-limiting example, the sequence accessible through the following database accession no.

giII710216 (all **information** available through the recited **accession** number is
In
incorporated herein by reference) which is described therein as "unknown [Homo sapiens...a polypeptide of the invention or a cell expressing such peptide. Once an
In
immune **response** is detected, e.g., antibodies specific for the antigen are detected in the mouse serum...

4/3,K/22 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00488451 **Image available**
INTEGRATED CUSTOMER INTERFACE FOR WEB BASED COMMUNICATIONS NETWORK MANAGEMENT
INTERFACE CLIENT INTEGREE POUR LA GESTION DE RESEAUX DE COMMUNICATIONS BASES SUR LE WEB
Patent Applicant/Assignee:
BARRY B Reilly,
CHODORONEK Mark A,
DEROSE Eric,
GONZALES Mark N,
JAMES Angela R,
LEVY Lynne,
TUSA Michael,
Inventor(s):
BARRY B Reilly,
CHODORONEK Mark A,
DEROSE Eric,
GONZALES Mark N,
JAMES Angela R,
LEVY Lynne,
TUSA Michael,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9919803 A1 19990422
Application: WO 98US20173 19980925 (PCT/WO US9820173)
Priority Application: US 9760655 19970926
Designated States: AU BR CA JP MX SG AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 90769

Fulltext Availability:

Detailed Description

Detailed Description
... some further authentication, they are free to retrieve the COUser object, and perform whatever special **authentication** they need, without troubling the user to re-enter his/her username and password. During...all order entry and security information for the "networkMCI Interact" suite of applications.

The security **information** which the StarOE maintains and provides describes **identification** , authentication and **access** control used in the suite of applications. All access to the "networkMCI Interact" is controlled...server 39 to the requesting systems and processes. An example of an output is an **authentication response** to the client side of the individual applications, e.g., call manager 1100, priced reporting...

4/3,K/23 (Item 16 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2003 WIPO/Univentio. All rts. reserv.

00473016 **Image available**
A CAMERA WITH INTERNAL PRINTING SYSTEM
APPAREIL PHOTOGRAPHIQUE A SYSTEME D'IMPRESSION INTERNE
Patent Applicant/Assignee:
SILVERBROOK RESEARCH PTY LIMITED,
SILVERBROOK Kia,
WALMSLEY Simon,
LAPSTUN Paul,
Inventor(s):
SILVERBROOK Kia,
WALMSLEY Simon,
LAPSTUN Paul,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9904368 A1 19990128
Application: WO 98AU544 19980715 (PCT/WO AU9800544)
Priority Application: AU 978003 19970715; AU 978005 19970715; AU 978031 19970715; AU 977991 19970715; AU 977998 19970715; AU 977988 19970715; AU 977993 19970715; AU 978012 19970715; AU 978017 19970715; AU 978014 19970715; AU 978025 19970715; AU 978032 19970715; AU 977999 19970715; AU 978024 19970715; AU 978016 19970715; AU 978030 19970715; AU 977938 19970715; AU 977997 19970715; AU 977979 19970715; AU 978015 19970715; AU 977978 19970715; AU 977982 19970715; AU 977989 19970715; AU 978019 19970715; AU 977980 19970715; AU 977942 19970715; AU 978018 19970715; AU 978021 19970715; AU 978000 19970715; AU 977940 19970715; AU 977939 19970715; AU 978020 19970715; AU 977985 19970715; AU 977987 19970715; AU 978022 19970715; AU 978029 19970715; AU 978023 19970715; AU 978028 19970715; AU 978027 19970715; AU 978026 19970715; AU 977983 19970715; AU 977986 19970715; AU 977981 19970715; AU 977977 19970715; AU 977934 19970715; AU 977990 19970715; AU 978497 19970811; AU 978505 19970811; AU 978498 19970811; AU 978504 19970811; AU 978501 19970811; AU 978500 19970811; AU 978502 19970811; AU 978499 19970811; AU 979395 19970923; AU 979404 19970923; AU 979394 19970923; AU 979396 19970923; AU 979397 19970923; AU 979398 19970923; AU 979399 19970923; AU 979400 19970923; AU 979401 19970923; AU 979402 19970923; AU 979403 19970923; AU 979405 19970923; AU 97959 19971216; AU 981397 19980119; AU 982370 19980316; AU 982371 19980316; AU 984094 19980612

Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 191348

Fulltext Availability:
Detailed Description

Detailed Description
... marks 1 109, borders 1 1 1 0, and targets 1 1 1 1. The **data** recrion holds the **encoded** **data** proper, while the clock-marks, borders and targets are present specifically to help locate the...

...thus becomes a black line with white on either side, making for a good frequency **response** on reading. The clockmarks alternating between white and black

4/3,K/24 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00456834 **Image available**
A SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR SWITCHED TELEPHONY COMMUNICATION
SYSTEME PROCEDE ET ARTICLE CONCU POUR LES COMMUNICATIONS TELEPHONIQUES PAR RESEAU COMMUTE
Patent Applicant/Assignee:
MCI WORLDCOM INC,
Inventor(s):
ZEY David A,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9847298 A2 19981022
Application: WO 98US7927 19980415 (PCT/WO US9807927)
Priority Application: US 97835789 19970415; US 97834320 19970415
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 156638
Fulltext Availability:
Detailed Description

Detailed Description
... be helpful to establish some terms.
ISP Intelligent Services Platform
NCS Network Control System
DAP **Data** **Access** Point
20 ACD Automatic Call Distributor
ISN Intelligent Services Network (Intelligent Network)
ISNAP Intelligent Services...IP.

*Configuration Data,%,
1) PC Online
Calculate

Search Report from Ginger D. Roberts

Challenge Challenge
2) Directory Service
Challenge calculat
Resvens: **Response**
3) **Challenge Response**
Authenticatfe user
U ate
pd
Pro Ile with Ep
4) PC Online Ack Ack, *Securitv Key...